Soluzioni algebra 1

gabriele.danieli.peluso

September 2023

1 Soluzioni foglio 1

Soluzione 1.1. Sono tutte vere da sinistra a destra, ma solo il terzo viceversa è vero. Per poter invertire le prime due e l'ultima è necessario che a, b siano coprimi. Le dimostrazioni sono banali.

Soluzione 1.2. La dimostrazione è assolutamente banale

Soluzione 1.3. I due sottogruppi sono meglio descritti come l'insieme dei multipli di n e l'insieme dei multipli di m. La loro intersezione pertanto è l'insieme dei numeri che vengono divisi da entrambi, tuttavia un numero è multiplo di due interi se e solo se è multiplo del loro minimo comune multiplo. Pertanto l'intersezione è $mcm(n, m)\mathbb{Z}$.

Soluzione 1.4.

1. La scrittura più ovvia in termini di generatori e relazioni è $C_{12} = \langle x | x^{12} \rangle$.
2. I sottogruppi non banali sono generati da un elemento di C_{12} che dividono 12, pertanto sono generati da $2, 3, 4, 6$ e sono quindi $G_2 = \{0, 2, 4, 6, 8, 10\}, G_3 = \{0, 3, 6, 9\}, G_4 = \{0, 4, 8\}, G_6 = \{0, 6\}$.
3. Per commutatività le classi laterali destre e sinistre coincidono. Quelle di G_2 sono $0 + G_2 = G_2$ e $1 + G_2 = \{1, 3, 5, 7, 9, 11\}$, quelle di G_3 sono $0 + G_3 = G_3$, $1 + G_3 = \{1, 4, 7, 10\}$, $2 + G_3 = \{2, 5, 8, 11\}$, quelle di G_4 sono $0 + G_4 = G_4$, $1 + G_4 = \{1, 5, 9\}, 2 + G_4 = \{2, 6, 10\}, 3 + G_4 = 3, 7, 11\}$. Infine quelle di G_6 sono $0 + G_6 = G_6, 1 + G_6 = \{1, 7\}, 2 + G_6 = \{2, 8\}, 3 + G_6 = \{3, 9\}, 4 + G_6 = \{4, 10\}, 5 + G_6 = \{5, 11\}$.
4. Per commutatività tutti i sottogruppi sono normali.
5. In generale per ogni sottogruppo notiamo che le classi laterali si sommano in modo usuale $x + G_y + z + G_y = (x + z) + G_y$ e quindi in ogni caso il quoziente $\mathbb{Z}_{12}/G_x \simeq \mathbb{Z}/x\mathbb{Z} \simeq \mathbb{Z}_x$

Soluzione 1.5.

1. Hanno lo stesso ordine.
2. Nulla, può persino essere che il prodotto abbia ordine infinito, ad esempio due riflessioni nel piano rispetto a due rette che formano angolo θ hanno entrambe ordine 2, ma componendole si ottiene una rotazione di angolo 2θ che con scelte opportune dell'angolo rende tutto incontrollabile.
3. Hanno lo stesso ordine.
4. I primi tre hanno lo stesso ordine, L'ultimo invece è incontrollabile, infatti basta riapplicare il ragionamento fatto sopra con $z = id$. In generale l'ordine si mantiene quando si opera ciclicamente, ossia si trasporta un termine dalla prima all'ultima "casella" ma si rompe completamente quuando si effettua uno scambio fra "caselle".
5. risulta essere esattamente $n/MCD(n, r)$.

6. Sicuramente $x^{rn} = id$ ma questo non vuol dire che l'ordine sia necessariamente rn. Infatti l'ordine è la più piccola potenza che riporta all'identità. Ad esempio in $\mathbb{Z}_5$ con l'operazione di prodotto gli elementi $2, 3$ hanno ordine 4 ma $3 \equiv_5 2^3$. Sicuramente si può dire che l'ordine m divida rn, altrimenti se $x^m = x^{rn} = id$ potrei eseguire la divisione euclidea $rn = mq + r$ ed avere $id = x^{rn} = x^{mq}x^r = (x^m)^q x^r = (id)^q x^r = x^r$. Ottenendo quindi una potenza più piccola dell'ordine che riporta x all'identità. Assurdo per definizione di ordine. In generale se $x^m = id$ l'ordine di x deve necessariamente dividere m per lo stesso ragionamento.

7. Se $x^n = id, y^m = id$ allora varrebbe che $(xy)^{mcm(m,n)} = x^{mcm(m,n)}y^{mcm(m,n)} = id$, quindi per il ragionamento di sopra l'ordine del prodotto divide il minimo comune multiplo degli ordini. Tuttavi potrebbe essere più piccolo, ad esempio in $\mathbb{Z}_9$ con l'operazione di prodotto l'elementi $2, 5$ hanno ordine 6 (provare per credere) mentre $2 \cdot 5 = 1$ quindi il prodotto ha ordine 1.

Soluzione 1.6. La dimostrazione che sia un gruppo è assolutamente banale, l'isomorfismo fra $(G, \cdot)$ e $(G, \circ)$ è la funzione $f : g \mapsto g^{-1}$ questa è tale che $f(g \cdot h) = (g \cdot h)^{-1} = h^{-1} \cdot g^{-1} = g^{-1} \circ h^{-1} = f(g)f(h)$ ed è ovviamente biettiva.

2 Soluzioni foglio 2

Soluzione 2.1. Dati $x, y \in G$ vale che xy ha ordine 2, quindi $xyxy = id$ e moltiplicando prima per y, poi per x a destra otteniamo $xy = yx$.

Soluzione 2.2. Molto banalmente se il sottogruppo $H < G$ possiede metà elementi allora la classe dell'identità è uguale sia a sinistra che a destra e coincide con H, questo vuol dire che l'altra metà degli elementi formano sia la classe laterale sinistra che quella destra visto che le classi laterali hanno sempre lo stesso numero di elementi. Se avesse un terzo degli elementi no si può dire nulla, ad esempio S_3 con il sottogruppo $\{id, (12)\}$ ha classi laterali distinte.

Soluzione 2.3.

1. Ha 8 elementi, infatti l'ultima relazione stabilisce una quasi commutatività $xy = yx^{-1}$ da cui si evince che gli elementi possono tutti essere scritti nella forma $id, x, x^2, x^3, y, yx, yx^2, yx^3$ e qualsiasi prodotto fra questi elemnti può essere ricondotto in questa forma "spostando" le y a sinistra a prezzo di invertire le x che incontra.

2. Bisogna osservare che se un sottogruppo possedesse entrambi i generatori sarebbe banalmente tutto il gruppo! Quindi nello stesso sottogruppo non possono esserci x, y. Questo vuol dire che ne abbiamo uno generato da ogni elemento del gruppo:

$$G_x = \{id, x, x^2, x^3\}, G_y = \{id, y\}, G_{xy} = \{id, xy\}$$

$$G_{yx^2} = \{id, yx^2\}, G_{yx^3} = \{id, yx^3\}, G_{x^2} = \{id, x^2\}$$

   ed uno particolare ne abbiamo uno generato da y, x^2 che denoteremo $K = \{id, x^2, y, yx^2\}$.

3. Per G_x che contiene metà elementi sappiamo dall'esercizio sopra che le classi laterali sinistre e destre coincidono e sono pari a $idG_x = G_x, yG_x = \{y, yx, yx^2, yx^3\}$. Per G_{x^2} notiamo che x^2 commuta con x ed y, pertanto anche per questo le classi laterali sinistre e destre coincidono e sono: $idG_{x^2} = G_{x^2}, xG_{x^2} = \{x, x^3\}, yG_{x^2} = \{y, yx^2\}, yxG_{x^2} = \{yx, yx^3\}$. Invece per G_y le classi laterali sono diverse, infatti abbiamo $xG_y = \{x, yx^3\} \neq G_yx = \{x, yx\}, x^3G_y = \{x^3, yx\} \neq G_yx^3 = \{x^3, yx^3\}$, mentre l'ultima classe laterale è uguale $x^2G_y = G_yx^2 = \{x^2, yx^2\}$. Infine K contiene metà elementi ed ha le classi laterali coincidenti che sono $idK = K, xK = \{x, yx, x^3, yx^3\}$. Senza dilungarsi in dettagli si nota che i gruppi rimanenti non sono normali.

4. I sottogruppi normali sono quindi $G_x, G_{x^2}K$.

5. Poiché G_x e K hanno metà elementi il quoziente ne ha solo due e risulta quindi essere isomorfo a $\mathbb{Z}_2$. Invece per D_4/G_{x^2} notiamo che quozientare per G_{x^2} significa aggiungere la relazione $x^2 = id$, pertanto il gruppo quiziente è scritto in termini di generatori e relazioni come $D_4/G_{x^2} = \langle x, y | x^2, y^2, xyxy \rangle$. Ovvero risulta isomorfo al gruppo di Klein.

Soluzione 2.4. 1. Ne abbiamo uno generato da ogni unità immaginaria:

$$G_i = \{1, i, -1, -i\}, G_j = \{1, j, -1, -j\}, G_k = \{1, k, -1, -k\}$$

più un altro generato da $-1, G_{-1} = \{1, -1\}$.

2. I primi tre gruppi hanno metà elementi quindi le classi laterali coincidono e come oramai è chiaro l'unica classe laterale per ogni gruppo comprende l'altra metà degli elementi. Per l'ultimo invece notiamo che $1, -1$ commutano con tutto il gruppo, quindi anche per questo gruppo le classi laterali coincidono e sono: $1G_{-1} = G_{-1}, iG_{-1} = \{\pm i\}, jG_{-1} = \{\pm j\}, kG_{-1} = \{k\}$.

3. Da sopra emerge che tutti i sottogruppi sono normali.

4. Come precedentemente quando quozientiamo per metà degli elementi otteniamo un gruppo con due elementi e quindi non possiamo che ottenere $\mathbb{Z}_2$, invece quando quozientiamo per il secondo notiamo che nel quoziente identifichiamo -1 a 1, perciò otteniamo che $i^2 = j^2 = k^2 = 1$. Da cui si evince che il quoziente è un gruppo con 4 elementi di ordine due. Risulta pertanto essere il gruppo di Klein.

Soluzione 2.5. Anzitutto è un morfismo perché $hk \mapsto g^{-1}hkg = g^{-1}hgg^{-1}kg$, quindi rispetta la composizione degli elementi. Successivamente è iniettivo perché $g^{-1}hg = 1 \Leftrightarrow h = 1$. Infine è suriettivo perché l'elemento k è raggiunto dall'elemento gkg^{-1}.

Soluzione 2.6. Supponiamo per assurdo che non esista alcun elemento di ordine pari in G, questo vorrebbe dire che ogni elemento ha ordine dispari. Preso allora un insieme di generatori $g_1, \cdots g_n$ di ordini $k_1, cdots, k_n$ dispari, ognuno genera $k_i - 1$ elementi più l'identità. Questo vorrebbe dire che G ha $1 + \sum_{i=1}^{n}(k_i - 1)$ che è un numero dispari. Vi è anche la possibilità che lo span di un elemento si intersechi con un altro e se per qualche indice dovesse valere $g_i^n = g_j^m = h$ allora dall'ipotesi assurda varrebbe che h ha ordine dispari, quindi nel conteggio sopra dovremmo togliere una copia dello span di h meno l'identità che abbiamo contato due volte. Ma ciò corrisponde a togliere un numo pari di elementi, quindi otterremo ancora che G ha un numero dispari di elementi. Iterando questo ragionamento otteniamo un assurdo. Quindi sia ora g di ordie pari $g^{2n} = id$ allora banalmente g^n ha ordine 2.

3 Soluzioni foglio 3

Soluzione 3.1. 1. è riflessiva poiché $idgg^{-1} = g$, è simmetrica poiché se $kgk^{-1} = h \Rightarrow g = k^{-1}hk$ ed è transitiva visto che se $kgk^{-1} = h, aha^{-1} = b \Rightarrow akg(ak)^{-1} = b$.

2. Se $kgk^{-1} = h \Rightarrow kg^nk^{-1} = h^n$, in particolare se per una potenza uno dei due termini raggiunge l'identità allora anche l'altro deve essere l'identità. Quindi due elementi coniugati hanno lo stesso ordine.

3. Anzitutto bisogna osservare che l'identità è coniugata solo a se stessa visto che $gidg^{-1} = id$, l'unica possibilità affinchè le classi abbiano lo stesso numero di elementi è che ogni altro elemento sia coniugato a se stesso, ma ciò vorrebbe dire che $\forall g, h \in G ghg^{-1} = h \Leftrightarrow gh = hg$. In altre parole le classi di coniugio hanno lo stesso numero di elementi se e solo se il gruppo è commutativo.

Soluzione 3.2. 1. In generale per ogni sottogruppo di $\mathbb{Z}_n$ notiamo che le classi laterali si sommano in modo usuale $x + G_y + z + G_y = (x + z) + G_y$ e quindi in ogni caso il quoziente $\mathbb{Z}_{12}/G_x \simeq \mathbb{Z}/x\mathbb{Z} \simeq \mathbb{Z}_x$ usando il teorema degli isomorfismi.

2. Poiché G_x e K hanno metà elementi il quoziente ne ha solo due e risulta quindi essere isomorfo a $\mathbb{Z}_2$. Invece per D_4/G_{x^2} notiamo che quozientare per G_{x^2} significa aggiungere la relazione $x^2 = id$, pertanto il gruppo quiziente è scritto in termini di generatori e relazioni come $D_4/G_{x^2} = \langle x, y | x^2, y^2, xyxy \rangle$. Ovvero risulta isomorfo al gruppo di Klein.

3. Come precedentemente quando quozientiamo per metà degli elementi otteniamo un gruppo con due elementi e quindi non possiamo che ottenere $\mathbb{Z}_2$, invece quando quozientiamo per il secondo notiamo che nel quoziente identifichiamo -1 a 1, perciò otteniamo che $i^2 = j^2 = k^2 = 1$. Da cui si evince che il quoziente è un gruppo con 4 elementi di ordine due. Risulta pertanto essere il gruppo di Klein.

Soluzione 3.3. 1. L'idea è che se permutassi le colonne di una matrice il determinante cambia quando eseguo un numero dispari di trasposizioni, quindi rimane inalterato se si effettuano un numero pari di permutazioni. Da ciò si evince che:

$$A_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Dove la permutazione (123) ad esempio è da intendersi come la permutazione che porta la prima colonna nella seconda, la seconda nella terza, la terza nella prima e lascia al suo posto la quarta. Inoltre risulta essere un sottogruppo perché la composizione di due permutazioni che non cambiano il determinante ovviamente non cambia il determinante e se per assurdo una permutazione non cambia il determinante e la sua inversa sì allora la composizione (che è la permutazione identità) cambierebbe il determinante, cosa assurda.

2. Il numero minimo è due, infatti ogni volta che prendiamo un elemento di ordine tre ed uno di ordine 2 il sottogruppo generato può avere 6 o 12 elementi. Se ne avesse 6 vi sono due possibilità: esso è isomorfo a C_6 oppure ad S_3. La prima ipotesi è da escludere visto che A_4 non ha elementi di ordine 6 mentre la seconda è anche da escludere visto che S_3 ha l'identità, un tre ciclo di ordine e tre elementi di ordine 2, tuttavia un rapido conto mostra che questa ipotesi non crea mai un sottogruppo di ordine 6. Analogamente se un sottogruppo avesse due elementi di ordine tre allora potrebbe avere 3,6 o 12 elementi. Se i due elementi fossero non appartenenti allo stesso ciclo potremmo escludere le prime due ipotesi in modo ovvio.

3. Abbiamo sicuramente i sottogruppi generati dai singoli elementi, ma a parte questi ve ne è anche un'altro $K = \{id, (12)(34), (13)(24), (14)(23)\}$ isomorfo al gruppo di Klein. Non ve ne sono altri per le ragioni espresse sopra.

4. L'unico sottogruppo normale è K

5. Il quoziente ha tre elementi, perciò $A_4/K \simeq \mathbb{Z}_3$

Soluzione 3.4. 1. Nel primo caso bisogna scegliere dove mandare il generatore di $\mathbb{Z}$, e lo possiamo mandare senza alcun problema in ognuno degli n elementi di $\mathbb{Z}_n$, abbiamo quindi n morfismi indicizzati da $f_n : \mathbb{Z} \to \mathbb{Z}_n | f(1) = n$.

Il viceversa invece è impossibile visto che gli elementi di $\mathbb{Z}_n$ hanno ordine finito devo mandarli tutti nell'unico elemento di Z che ha ordine finito, ovvero lo 0, perciò vi è solo il morfismo banale che manda tutto in 0.

2. In questo caso non convienere ragionare in termine di generatori poiché rispettare le relazioni di A_4 sarebbe in un vero inferno, conviene chiedersi quali sono i possibili kernel e visto che devono essere sottogruppi normali ho solo tre possibilità: due sottogruppi banali e $K = \{(12)(34), (13)(24), (14)(23), id\}$. Visto che A_4 ha 12 elementi ed Q_8 ne ha 8 il kernel non può essere banale, questo vorrebbe dire che un morfismo non banale dovrebbe avere $ker = K$ ma A_4/K ha 3 elementi e Q_8 non ha sottogruppi di tre elementi. Quindi c'è solo il morfismo banale.

Per il viceversa notiamo ancora non possono essere isomorfi per ragioni di cardinalità, quindi a parte il morfismo banale ho 4 possibili kernel: il sottogruppo di due elementi G_{-1} e tre

sottogruppi da 4 elementi generati dalle unità immaginarie G_i, G_j, G_k. Per G_{-1} notiamo che $Q_8/G_{-1} \approx K$ e potrò quindi scegliere dove mandare le tre unità immaginarie dentro K avendo 6 scelte diverse. Invece se il kernel fosse uno dei gruppi daa quattro elementi varrebbe che $Q_8/G_i \approx \mathbb{Z}_2$ ed ho tre scelte su dove mandare l'elemento di ordine 2. Quindi in totale avrei altri 9 morfismi, per un totale di 16 morfismi.

3. Per ragioni di ordine il nucleo di questo morfismo deve avere almeno 4 elementi, abbiamo quindi come kernel K, G_x ed in entrambi i casi il quoziente è un gruppo di due elementi determinato solo dall'elemento di ordine due in S_3 in cui va a finire la classe non banale, abbiamo quindi 2 scelte per il kenrel e 3 scelte dell'immagine, 6 morfismi più uno banale.

   Per il viceversa vale un ragionamento simile, l'unico kernel è C_3 e quindi l'immagine deve essere scelta fra gli elementi di ordine 2 in D_4 avendo 2 sole scelte possibili.

Soluzione 3.5. Scrivendo $k = ak$ ed usando il secondo teorema di isomorfismo con i gruppi $G = \mathbb{Z}, H = h\mathbb{Z}, N = a\mathbb{Z}$ vale che $H \cap N = k\mathbb{Z}$. Allora il gruppo considerato sarebbe $H/H \cap N$ che dal teorema è isomorfo a $G/N = \mathbb{Z}/a\mathbb{Z} = \mathbb{Z}_a$.

4 Soluzioni foglio 4

Soluzione 4.1. 1. Anzitutto per commutatività gli automorfismi interni sono sempre identici. Poi $\mathbb{Z}$ ha solo due generatori, ± 1, quindi un automorfismo può solo lasciare tutto così com'è o invertirli. Perciò vi sono solo due automorfismi, quindi $Aut(\mathbb{Z}) \approx \mathbb{Z}_2$.

2. Come prima per commutatività gli automorfismi interni sono identici. Successivamente la domanda da porci è dove mandare il generatore $1 \in \mathbb{Z}_n$. Ovviamente deve andare in un altro generatore $m \in \mathbb{Z}_n$ coprimo con n. Se chiamiamo tale morfismo f_m deve valere che $f_m(x) = mx$. Da cui capiamo che la composizione fra due morfismi rappresenta un prodotto $f_m \circ f_l = f_{ml}$. Da ciò è chiaro che $Aut(\mathbb{Z}_n) \approx (\mathbb{Z}_n, \cdot)$. Ovvero gli automorfismi sono $\mathbb{Z}_n$ inteso come gruppo moltiplicativo.

3. Osserviamo che il centro di D_4 contiene il solo elemento x^2 e $D_4/\{id, x^2\} \approx K$ Quindi $Inn(D_4) \approx K$. Ora mostriamo che non può avere altri elementi: D_4 ha due generatori, x ha ordine 4 e può deve essere mandato in uno dei 2 elementi di ordine 4: x, x^3. Invece y ha ordine 2 e può essere mandato in y, yx, yx^2, yx^3, non può andare in x^2 altrimenti non sarebbe suriettivo. Quindi a priori ci sono otto scelte di permutazione, quindi a priori $Aut(D_4)$ potrebbe avere 8 elementi. Osserviamo però che una scelta è incompatibile, ad esempio se $x \mapsto x, y \mapsto yx$ allora la relazione $id = xyxy \mapsto xyxxyx = xyx^2yx = xyyx = x^2 \neq id$. Quindi $Aut(D_4)$ ha meno di 8 elementi ma ha un sottogruppo con 4 elementi e poiché 4 deve dividere il numero di elementi l'unica possibilità è che tutti gli automorfismi siano interni.

4. Il centro di Q_8 è $\{\pm 1\}$, quindi gli automorfismi interni sono $Q_8/\{\pm 1\} \approx K$. Questi automorfismi interni agiscono sui generatori come ad esempio $Ad_i(i) = i, Ad_i(j) = -j, Ad_i(k) = -k$ ed in generale si osserva che le mappe aggiunte di una unità immaginara tengono fissa quella ma cambiano il segno alle altre due. Osserviamo però che vi possono essere altri automorfismi, ad esempio cambiando ciclicamente le unità immaginarie $i \mapsto j, j \mapsto k, k \mapsto i$ otterremo comunque un automorfismo, così come se permutassimo e scambiassimo un segno $i \mapsto j, j \mapsto i, k \mapsto -k$. Queste due trasformazioni generano un sottogruppo di permutazioni sulle unità immaginarie isomorfo a S_3 che non si interseca con il K dato dagli isomorfismi interni, quindi il sottogruppo generato da tutti e due ha 24 elementi. Tuttavia queste sono le uniche scelte visto che ho 6 scelte su dove mandare un generatore, 4 scelte su dove mandare il secondo ed a quel punto la ciclicità fissa il terzo generatore, quindi il gruppo degli automorfismi ha al più 24 elementi. Visto che il sottogruppo degli automorfismi interni è normale possiamo scrivere sicuramente $Aut(Q_8) = K \times S_3$ come prodotto semidiretto (non so fare il simbolo del prodotto semidiretto il latex) (Si può dimostrare che questo prodotto semidiretto è ulteriormente isomorfo a S_4).

5. Poiché il centro di A_4 è banale gli automorfismi interni sono isomorfi a $A_4/\{id\} \approx A_4$. Osserviamo però che anche se coniugassi con un elemento di S_4 le cose andrebbero bene, visto che eseguirei una composizione fra due permutazioni che cambiano il determinante ed una che non lo cambia. Questo induce un morfismo iniettivo $f : S_4 \to Aut(A_4)|f_\sigma(\tau) = \sigma\tau\sigma^{-1}$. In totale quindi $Aut(A_4)$ avrebbe almeno 24 automorfismi. Tuttavia non può averne di più visto che A_4 può essere generato da un elemento di ordine 3 ed uno di ordine 2. Essendoci 8 elementi di ordine 3 e 3 di ordine 2 non possono esserci più di $24 = 8 \cdot 3$ scelte totali.

Soluzione 4.2. 1. Poichè $Imm(i) = Ker(\pi)$ quel sottogruppo è il kernel di un morfismo, quindi è un sottogruppo normale dal teorema di omomorfismo. Il resto è esattamente l'enunciato del teorema sui morfismi.

2. Se la sequenza si spezzasse con il morfismo j tale che $\pi \circ j = Id_K$ allora j deve essere iniettivo o la proprietà precedente non potrebbe valere. Quindi j è un isomorfismo con l'immagine, cioé esiste un sottogruppo di G isomorfo a K e possiamo scrivere senza perdere tempo nei dettagli $Imm(j) < G$. Inoltre se esistesse un elemento $g \in Imm(K) \cap Imm(H), g = j(k) = i(h)$ allora applicando π a tutte le uguaglianze avremmo: $\pi(g) = \pi(i(h)) = \pi(j(k))$ da cui: $\pi(g) = id = k$. Quindi dalle ultime due $g = j(id) = id$. Ovvero $Imm(i) \cap Imm(j) = \{id\}$. Inoltre $Imm(i) \cdot Imm(j) = G$, altrimenti il quoziente $G/Imm(i)$ avrebbe più elementi del solo K. Essendo $Imm(i)$ normale possiamo concludere che $G = Imm(j) \ltimes_\phi Imm(i)$ per qualche omomorfismo $\phi : Imm(j) \to Aut(Imm(i))$ dato dal coniugio degli elementi di $Imm(i)$.

   Viceversa se $G = K \ltimes_\phi H$ allora preso i immersione di H in G, π la proiezione al quoziente $G \to G/H = K$ e j immersione di K in G otteniamo banalmente una sequenza esatta corta spezzata.

Soluzione 4.3. Consideriamo la funzione $(h, k) \mapsto (f(h), g(k))$, allora vale che:

$$(h_1, k_1) \times_\phi (h_2, k_2) = (h_1 h_2, \phi_{h_2}(k_1)k_2) \mapsto (f(h_1)f(h_2), g(\phi_{h_2}(k_1))g(k_2)$$

mentre

$$(f(h_1), g(k_1)) \times_\psi (f(h_2), g(k_2)) = (f(h_1)f(h_2), \psi_{f(h_2)}(g(k_1))g(k_2))$$

ma dall'uguaglianza espressa nella consegna emerge che:$\psi_{f(h_2)}(g(k_1)) = g(\phi_{h_2}(k_1))$, quindi la funzione sopra è un morfismo e la biettività segue dal fatto che f, g sono isomorfismi sui singoli sottogruppi.

Soluzione 4.4. 1. Gli unici sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$ che portano a quozienti $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ ma è impossibile spezzare queste sequenze visto che nessun elemento di $\mathbb{Z}$ ha ordine finito. Quindi non è possibile scrivere $\mathbb{Z}$ come prodotto diretto o semidiretto.

2. Sappiamo che $\mathbb{Z}_n, \mathbb{Z}_m$ si immergono in $\mathbb{Z}_{nm}$ e che l'immersione $\mathbb{Z}_n \to \mathbb{Z}_{nm}, x \mapsto mx$ è iniettiva. Sappiamo anche che il quoziente deve essere $\mathbb{Z}_{nm}/\mathbb{Z}_n = \mathbb{Z}_m$. Il problema è che per spezzare la sequenza non possiamo usare l'immersione analoga $\mathbb{Z}_m \to \mathbb{Z}_{nm}, y \to ny$ visto che la proiezione manda $1 \in \mathbb{Z}_{nm} \mapsto 1 \in \mathbb{Z}_m$. Questo vuol dire che per spezzare la sequenza dobbiamo mandare $1 \in \mathbb{Z}_m$ in un elemento di ordine m in $\mathbb{Z}_{nm}$ che appartenga alla classe laterale $1 + \mathbb{Z}_n \subset \mathbb{Z}_{nm}$. In altre parole dobbiamo mandarlo in un elemento x che soddisfa il sistema:

$$\begin{cases} mx \equiv_{nm} 0 \\ x \equiv_m 1 \end{cases} \quad \text{ovvero} \quad \begin{cases} x \equiv_n 0 \\ x \equiv_m 1 \end{cases}$$

   Questo sistema ha soluzione se e solo se n, m sono coprimi.

3. Sappiamo che D_n ha come sottogruppo normale $\mathbb{Z}_n$ e che il quoziente deve esere $\mathbb{Z}_2$ visto che è un gruppo da due elementi. Per spezzare la sequenza basta mandare l'elemento non banale di $\mathbb{Z}_2$ nell'elementi $y \in D_n$ e questo ci dice che $D_n = \mathbb{Z}_2 \ltimes \phi\mathbb{Z}_n$ con automorfismo $\phi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n)$ che porta l'elemento non banale di $\mathbb{Z}_2$ nell'automorfismo di $\mathbb{Z}_n$ che porta $x \mapsto -x$.

4. Sappiamo che S_3 ha come sottogruppo normale $\mathbb{Z}_3 = \{id, (123), (132)\}$ ed il quoziente deve essere $S_3/\mathbb{Z}_3 = \mathbb{Z}_2$ che si spezza mandando l'elemento non banale di $\mathbb{Z}_2$ in (12), da cui $S_3 = \mathbb{Z}_2 \ltimes \mathbb{Z}_3$.

5. Analogamente sappiamo che A_4 ha come sottogruppo normale K con quoziente $A_4/K = \mathbb{Z}_3$. Per spezzarla basta mandare il generatore di $\mathbb{Z}_3$ in (123), da cui $A_4 = \mathbb{Z}_3 \ltimes K$.

Soluzione 4.5. Le prime dimostrazioni sono assolutamente banali, per i controesempi invece bisogna ragionare un pochetto. Ad esempio sappiamo che $A_4 = \mathbb{Z}_3 \ltimes K = \mathbb{Z}_3 \ltimes (\mathbb{Z}_2 \ltimes \mathbb{Z}_2)$ dove l'ultimo prodotto in realtà è diretto ma non ci interessa. Tuttavia non può succedere che $A_4 = (\mathbb{Z}_3 \ltimes \mathbb{Z}_2) \ltimes \mathbb{Z}_2$ perché A_4 non ha sottogruppi normali di ordine 2. Analogamente non è commutativo perché $A_4 = \mathbb{Z}_3 \ltimes K$ ma non può valere che $A_4 = K \ltimes \mathbb{Z}_3$ perché A_4 non ha sottogruppi normali di ordine 3.

5 Soluzioni foglio 5

Soluzione 5.1. Sono tutte vere da sinistra a destra, ma solo il terzo viceversa è vero. Per poter invertire le prime due e l'ultima è necessario che a, b siano coprimi. Le dimostrazioni sono banali.

Soluzione 5.2. Scrivendo il numero come $x \cdot 10 + y$ vale che:

$$0 \equiv_7 x \cdot 10 + y \equiv_7 3 \cdot x + y \Leftrightarrow$$

$$-2 \cdot 0 \equiv_7 -2 \cdot 3 \cdot x - 2 \cdot y \Leftrightarrow$$

$$0 \equiv_7 x - 2y$$

Poiché $-6 \equiv_7 1$.

Soluzione 5.3. Cerchiamo due numeri h, k tali che $123k + 542h = 1$. Per trovarli procediamo con l'algoritmo euclideo delle divisioni successive:

$$542 = 4 \cdot 123 + 50 \quad 123 = 2 \cdot 50 + 23 \quad 50 = 2 \cdot 23 + 4 \quad 23 = 5 \cdot 4 + 3 \quad 4 = 3 + 1$$

E leggendole al contrario si ottiene:

$$1 = 4 - 3 = 4 - (23 - 4 \cdot 5) = -23 + 6(50 - 23 \cdot 2) = 6 \cdot 50 - 13(123 - 50 \cdot 2) =$$

$$= -13 \cdot 123 + 32 \cdot 50 = -13 \cdot 123 + 32(542 - 4 \cdot 123) = -141 \cdot 123 + 32 \cdot 542.$$

Da cui $-141 \cdot 123 \equiv_{542} 1$

Soluzione 5.4. Usando il primo esercizio possiamo accorpare diverse righe del sistema ottenendo:

$$\begin{cases} 2x \equiv_5 1 \\ 4x \equiv_7 1 \\ 7x \equiv_{11} 1 \end{cases} \Leftrightarrow \begin{cases} 14x + 20x \equiv_{35} 5 + 7 \\ 7x \equiv_{11} 1 \end{cases} \Leftrightarrow \begin{cases} -x \equiv_{35} 12 \\ 7x \equiv_{11} 1 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow -11x + 245x \equiv_{385} 35 + 132 \Leftrightarrow 234x \equiv_{385} 167$$

In altre parole dobbiamo trovare x, h con $234x + 385h = 167$. Per farlo operiamo con l'algoritmo euclideo delle divisioni successive fino ad ottenere (conti omessi):

$$1 = -51 \cdot 234 + 31 \cdot 385$$

da cui:

$$167 = -51 \cdot 167 \cdot 234 + 167 \cdot 31 \cdot 385$$

poiché $-51 \cdot 167 = -8517$ La soluzione è $x \equiv_{385} -8517 \equiv_{385} 338$.

Per il secondo sistema procediamo in modo analogo:

$$\begin{cases} 2x \equiv_{15} 3 \\ 3x \equiv_8 5 \\ 4x \equiv_7 2 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{15} -6 \\ x \equiv_8 -1 \\ x \equiv_7 4 \end{cases} \Leftrightarrow \begin{cases} x \equiv_{15} -6 \\ 15x \equiv_{56} 25 \end{cases} \Leftrightarrow 101x \equiv_{840} -261$$

Ancora una volta procediamo con l'algoritmo euclideo fino ad ottenere:

$$1 = 341 \cdot 101 - 41 \cdot 840 \Rightarrow -261 \equiv_{840} 101 \cdot 341 \cdot (-261) \Rightarrow x \equiv_{840} -89001 \equiv_{840} 39$$

Per quanto riguarda l'ultimo sistema notiamo che le equazioni modulari non sono coprime fra loro, perciò le dobbiamo prima spezzare:

$$\begin{cases} 7x \equiv_{12} 4 \\ 5x \equiv_{26} 6 \\ x \equiv_6 0 \end{cases} \Leftrightarrow \begin{cases} 7x \equiv_4 4 \\ 7x \equiv_3 4 \\ 5x \equiv_{13} 6 \\ 5x \equiv_2 6 \\ x \equiv_2 0 \\ x \equiv_3 0 \end{cases}$$

Da qui notiamo che il sistema è impossibile visto che l'ultima equazione implica che x sia un multiplo di 3 ma se ciò fosse vero la seconda riga sarebbe necessariamente falsa poiché $7x \equiv_3 0 \not\equiv_3 4$

Soluzione 5.5. Iniziamo osservando che le potenze di 2 in $\mathbb{Z}_{12}$ hanno l'andamento:

$$(2^0, 2^1, 2^2, 2^3, 2^4, 2^5 \cdots) = (1, 2, 4, 8, 4, 8, \cdots)$$

. Perciò l'unica soluzione è $x = 1$.

Per la seconda equazione osserviamo che le potenze di 3 in $\mathbb{Z}_{15}$ hanno l'andamento:

$$(3^0, 3^1, 3^2, 3^3, 3^4, 3^5, \cdots) = (1, 3, 9, -3, -9, 3, \cdots)$$

. Quindi vi sono infinite soluzioni del tipo $x \equiv_4 1, x > 0$.

Per il sistema a seguire ricordiamo che l'inverso di 2 modulo 5 è 3 e che l'ordine di 2 in $\mathbb{Z}_5$ è 4, ciò detto procediamo usando il primo esercizio:

$$\begin{cases} 2x \equiv_3 1 \\ 2^x \equiv_5 2^{-1} \end{cases} \Leftrightarrow \begin{cases} x \equiv_3 -1 \\ x + 1 \equiv_4 0 \end{cases} \Leftrightarrow x \equiv_{12} -1$$

Per l'ultimo sistema inizamo osservando alcuni fatti: anzitutto $-3 \equiv_8 5$, $3 \cdot 5 = 15 \equiv_7 1 \Rightarrow 5 \equiv_7 3^{-1}$ ed infine $2^5 = 32 \equiv_{25} 7$. Inoltre 5 ha ordine 2 in $\mathbb{Z}_8$, 2 ha ordine 20 in $\mathbb{Z}_{25}$ e 3 ha ordine 6 in $\mathbb{Z}_7$. Perciò il sistema diventa:

$$\begin{cases} 5^x \equiv_8 5 \\ 2^x \equiv_{25} 2^5 \\ 3^x \equiv_7 3^{-1} \end{cases} \Leftrightarrow \begin{cases} 5^{x-1} \equiv_8 1 \\ 2^{x-5} \equiv_{25} 1 \\ 3^{x+1} \equiv_7 1 \end{cases} \Leftrightarrow \begin{cases} x - 1 \equiv_2 0 \\ x - 5 \equiv_{20} 0 \\ x + 1 \equiv_6 0 \end{cases}$$

Spezzandole in equazioni coprime si ottiene:

$$\begin{cases} x \equiv_2 1 \\ x \equiv_4 1 \\ x \equiv_5 0 \\ x \equiv_2 1 \\ x \equiv_3 2 \end{cases} \Leftrightarrow \begin{cases} x \equiv_4 1 \\ x \equiv_5 0 \\ x \equiv_3 2 \end{cases}$$

Ed usando le formule risolutive standard (ma anche ad occhio) si ottiene che la soluzione è $x \equiv_{60} 5$.

Soluzione 5.6. Iniziamo studiando le potenze di 2 modulo 9 che sono: $2, 4, 8 \equiv_9 -1, 16 \equiv_9 7 \equiv_9 -2, 32 \equiv_9 5 \equiv_9 -4, 64 \equiv_9 1$. Quindi $2^n + 2^m \equiv_9 0 \Leftrightarrow 2^{n-m} \equiv_9 -1 \Leftrightarrow n - m \equiv_6 3$

Soluzione 5.7. Dobbiamo calcolare $x \equiv_{1000} 2023^{2102} \equiv_{1000} 23^{2102}$. Per farlo tuttavia è infinitamente più comodo spezzare l'uguaglianza in un sistema di equazioni modulari coprime:

$$\begin{cases} x \equiv_8 23^{2102} \\ x \equiv_{125} 23^{2102} \end{cases}$$

Vale che $23 \equiv_8 -1$ e che la funzione di eulero di 125 sia $\phi(125) = 100$. Perciò $23^{100} \equiv_{125} 1 \Rightarrow 23^{2100} \equiv_{125} 1$. Quindi il sistema diventa:

$$x \equiv_8 1x \equiv_{125} 23^2 = 529$$

Normalmente ora avremmo dovuto procedere il solito metodo risolutivo dei sistemi modulari ma fortunatamente $529 \equiv_8 1$, perciò possiamo scrivere usando ll'esercizio 1.1:

$$\begin{cases} x \equiv_8 529 \\ x \equiv_{125} 529 \end{cases} \quad \Leftrightarrow x \equiv_{1000} 529$$

Concludendo che le ultime tre cifre siano 529.

6 Soluzioni foglio 6

Soluzione 6.1. Sia $D = MCD(a^m - 1, a^n - 1)$. Poiché d divide m e n, si ha che $a^d - 1$ divide $a^m - 1$ e $a^n - 1$. Quindi $a^d - 1$ divide D. D'altra parte D divide $a^m - 1$, ovvero $a^m \equiv 1(D)$. Quindi $(a^m)^x \equiv 1(D)$, per ogni $x \in \mathbb{Z}$. Similmente, $(a^n)^y \equiv 1(D)$, per ogni $y \in \mathbb{Z}$. Dall'identità di Bezout si ha $a^d \equiv 1(D)$. Quindi D divide $a^d - 1$, da cui otteniamo $D = a^d - 1$.

Soluzione 6.2. Sia d un divisore di n. Allora $2^d - 1$ divide $2^n - 1$. Dato che $2^n - 1$ è primo, si ha soltanto $d = 1$ oppure $d = n$. Quindi n è primo.

Soluzione 6.3. Abbiamo

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)\,.$$

Dato che $a^{n-1} + a^{n-2} + \cdots + a + 1 > 1$ e $a^n - 1$ è primo, deve essere $a - 1 = 1$, ovvero $a = 2$. n è primo per l'esercizio precedente.

Soluzione 6.4. Se a è dispari, allora $a^n + 1$ è pari, dunque non può essere primo. Se $n = 2^k m$, con $m > 1$ dispari, allora $a^n + 1 = (a^{2k})^m - (-1)^m$, che è divisibile per $a^{2k} + 1$.

Soluzione 6.5. Abbiamo

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \ldots \frac{p-1}{2} \frac{p+1}{2} \ldots (p-2)(p-1) \\ &\equiv 1 \cdot 2 \ldots \frac{p-1}{2} \left(-\frac{p-1}{2}\right) \ldots (-2)(-1) \\ &\equiv (-1)^{p-1} \Big(\frac{p-1}{2}!\Big)^2 \equiv \Big(\frac{p-1}{2}!\Big)^2 \mod p\,. \end{aligned}$$

Il risultato segue dal Teorema di Wilson.

Soluzione 6.6.

1. Gruppo di Klein, composto dalle riflessioni attorno agli assi di simmetria più la simmetria centrale attorno l'origine.
2. Ancora il gruppo di Klein, composto dalle riflessioni attorno le due diagonali più la simmetria centrale attorno l'origine.

3. Il gruppo da due elementi composto dalla sola simmetria centrale.
4. Il gruppo S_3, generato dalla rotazione attorno al centro di 60 gradi e da una delle riflessioni attorno ad una altezza.
5. Il gruppo da due elementi composto dalla riflessione attorno all'asse di simmetria.
6. Il gruppo D_4, generato da una rotazione di 90 gradi attorno al centro più una riflessione attorno ad una diagonale.
7. Il gruppo D_n, generato da una rotazione di $360/n$ gradi più una riflessione attorno ad un asse di simmetria.
8. Il gruppo di Klein generato dalle riflessioni attorno gli assi dell'ellisse più la simmetria centrale attorno l'origine.
9. Ancora il gruppo di Klein generato dalle riflessioni attorno i due assi di simmetria più la simmetria centrale attorno l'origine.
10. Il prodotto semi-diretto $S^1 \rtimes \mathbb{Z}_2$, in cui il primo fattore rappresenta tutte le rotazioni di angolo θ ed il secondo fattore rappresenta una riflessione attorno ad uno degli infiniti assi di simmetria.

7 Soluzioni foglio 7

Soluzione 7.1. Ricordiamo che $\mathcal{M}_2 = \mathcal{T}_2 \rtimes \mathcal{O}_2$ e vale la regola di composizione $(T_a \circ \phi) \circ (T_b \circ \psi) = T_{a+\phi(b)} \circ \phi \circ \psi$, $T_a, T_b \in \mathcal{T}_2$, $\phi, \psi \in \mathcal{O}_2$. Per ipotesi $M = T_a \circ S_\ell$. quindi

$$M^2 = (T_a \circ S_\ell)^2 = T_{a+S_\ell(a)} \circ S_\ell^2 = T_{a+S_\ell(a)}\,,$$

dato che le riflessioni hanno ordine due.

Soluzione 7.2. Abbiamo visto a lezione che $T_a \circ R_\alpha$ è una rotazione intorno a p di angolo α. Quindi $\alpha = \theta$. Inoltre, p è definito dall'equazione $(T_a \circ R_\alpha)(p) = p$, da cui otteniamo che $a = (1 - R_\alpha)p$. La mappa cercata è

$$(p, \theta) \mapsto ((1 - R_\theta)p, \theta)\,,$$

che è invertibile poichè $\theta \neq 0$.

Soluzione 7.3. Abbiamo visto a lezione che $T_a \circ R_\alpha \circ S$ è una glissoriflessione. Per verificare che $S_{\ell,v} = T_a \circ R_\alpha \circ S$ dobbiamo far vedere che

$$(T_a \circ R_\alpha \circ S)(p) = p + v\,, \tag{7.1}$$

per ogni $p \in \ell$, dove a e α sono dati nel testo dell'esercizio. Usando la formula per a, riscriviamo il membro di sinistra di (7.1) come

$$(T_a \circ R_\alpha \circ S)(p) = (R_\alpha \circ S)(p) + v + \frac{2q}{1+m^2}\begin{pmatrix} -m \\ 1 \end{pmatrix}.$$

Quindi (7.1) è equivalente a

$$(R_\alpha \circ S)(p) - p = \frac{2q}{1+m^2}\begin{pmatrix} m \\ -1 \end{pmatrix}. \tag{7.2}$$

Scriviamo $p \in \ell$ come

$$p = p' + \begin{pmatrix} 0 \\ q \end{pmatrix}, \quad p' = \begin{pmatrix} 1 \\ m \end{pmatrix} t\,, \quad t \in \mathbb{R}\,.$$

Osserviamo che $p' \in \ell'$, dove ℓ' è la retta $y = mx$, che è la retta di riflessione di $R_\alpha \circ S$. Usando il fatto che $(R_\alpha \circ S)(p') = p'$ e la linearità di $R_\alpha \circ S$, l'equazione (7.2) è equivalente a

$$(1 + R_\alpha) \begin{pmatrix} 0 \\ q \end{pmatrix} = \frac{2q}{1+m^2} \begin{pmatrix} -m \\ 1 \end{pmatrix} .$$

Questa si verifica facilmente usando la formula per α e le identita'

$$\frac{2m}{1+m^2} = \sin\frac{\alpha}{2}\cos\frac{\alpha}{2} = \sin\alpha\,, \quad \frac{2}{1+m^2} = 2\cos^2\frac{\alpha}{2} = 1 + \cos\alpha\,.$$

Soluzione 7.4. Dall'Esercizio 2 sappiamo che

$$R_{p,\theta} = T_a \circ R_\theta\,, \quad a = (1 - R_\theta)p\,, \quad R_{q,\eta} = T_b \circ R_\eta\,, \quad b = (1 - R_\eta)q\,.$$

Usando la regola di composizione in $\mathcal{M}_2$ otteniamo

$$R_{p,\theta} \circ R_{q,\eta} = T_{a+R_\theta(b)} \circ R_{\theta+\eta}\,,$$

che è una traslazione se e soltanto se $R_{\theta+\eta} = 1$, quindi

$$\theta + \eta = 2k\pi\,, \quad k \in \mathbb{Z}\,.$$

Se $\theta+\eta = \pi$, allora $R_{\theta+\eta} = -1$ e usando l'Esercizio 1, il punto intorno al quale avviene la rotazione è

$$(1 - R_\pi)^{-1}(a + R_\theta(b)) = \frac{1}{2}(p + q - R_\theta(p - q))\,.$$

Soluzione 7.5. Dall'Esercizio 3 sappiamo che

$$S_{\ell,v} = T_a \circ R_\alpha \circ S\,, \quad \alpha = 2\arctan m_\ell\,, \quad S_{r,u} = T_b \circ R_\beta \circ S\,, \quad \beta = 2\arctan m_r\,.$$

Usando la regola di composizione in $\mathcal{M}_2$ otteniamo

$$S_{\ell,v} \circ S_{r,u} = T_{a+R_\alpha(S(b))} \circ R_{\alpha-\beta}\,,$$

che è una traslazione se e soltanto se $R_{\alpha-\beta} = 1$, quindi

$$\alpha - \beta = 2k\pi\,, \quad k \in \mathbb{Z}\,.$$

Ne segue che $m_\ell = m_r$, dunque ℓ e r sono rette parallele.

Soluzione 7.6. $R_{p,\frac{2\pi}{n}}$ è un elemento di ordine n, quindi $C_n(p) \simeq C_n$. Per la seconda affermazione è sufficiente far vedere che $C_n(p)$ e $C_n(0)$ sono coniugati. Basta prendere $g = T_p$. Il risultato segue dall'identità $T_p \circ R_\theta \circ T_{-p} = R_{p,\theta}$. Similmente si dimostra che $D_n(p,\ell) \simeq D_n$ per ogni retta del piano ℓ e $p \in \ell$. Per la seconda affermazione è sufficiente far vedere che $D_n(p,\ell)$ è coniugato a $D_n(p,\hat{x})$, dove $\hat{x}$ denota l'asse delle x. Basta prendere $g = R_{\theta,p} \circ T_p$. Il risultato segue dall'identità $R_\theta \circ S \circ R_{-\theta} = S_{R_\theta(\hat{x})}$.

8 Soluzioni foglio 8

Soluzione 8.1. Consideriamo il termine di sommatoria per primo e contiamolo in modo diverso:

$$\sum_{g\in G} |Fix(g)| = \sum_{g\in G} |\{(g,x) \in G \times X | g \cdot x = x\}| = |\{(g,x) \in G \times X | g \cdot x = x\}| =$$

$$= \sum_{x\in X} |\{(g,x) \in G \times X | g \cdot x = x\}| = \sum_{x\in X} |G_x| = |G| \sum_{x\in X} \frac{1}{O_x}$$

poiché per ogni stabilizzatore vale la relazione $|G| = |G_x||O_x|$. Tuttavia nella somma gli elementi della stessa orbita contribuiranno come 1, quindi alla fine della somma rimarranno solo tanti "uni" quante orbite, da cui.

$$\sum_{g\in G} |Fix(g)| = |G||X/G|$$

Soluzione 8.2. Prima di risolvere l'esercizio è necessario dimstrare un lemma preliminare: se $(a, n) = d$ allora esiste un $k \in \mathbb{N}$ coprimo con n tale che $kd \equiv_n a$. Infatti riscrivendo $a = \tilde{a}d, n = \tilde{n}d$ con $(\tilde{a}, \tilde{n}) = 1$ la condizione è equivalente a chiedere che $k \equiv_{\tilde{n}} \tilde{a}$. Questa equivalenza ci assicura che k non sia divisibile per ogni numero primo nella fattorizzazione di $\tilde{n}$. Invece per tutti i prim $p_1, \cdots p_l$ nella fattorizzazione di n che non compaiono nella fattorizzazione di $\tilde{n}$ possiamo aggiungere le condizioni:

$$\begin{cases} k \equiv_{\tilde{n}} \tilde{a} \\ k \equiv_{p_1} 1 \\ \vdots \\ k \equiv_{p_l} 1 \end{cases}$$

Che assicurano per il teorema cinese dei resti che esiste il k che cercavamo.

A seguire sappiamo che $Aut(\mathbb{Z}_n) = \mathbb{Z}_n^*$. Facciamolo agire per moltiplicazione $a \cdot x = ax$ su $\mathbb{Z}_n$. Sappiamo che la cardinalità del gruppo che agisce è pari al numero di elementi coprimi con n, ovvero $\phi(n)$. Sappiamo inoltre che il numero delle orbite dell'azione è pari al numero di divisori di n, infatti se se un elemento $x \in \mathbb{Z}$ ha massimo comun divisore d con n, allora moltiplicando x per un fattore coprimo con n otterrò un'altro elemento avente massimo comun divisore d con n. In modo usando il lemma di sopra si nota che l'azione è transitiva sul sottoinsieme di elementi con lo stesso massimo comun divisore con n. Quindi possiamo usare il lemma di Burnside:

$$d(n)\frac{1}{\phi(n)} \sum_{a \in \mathbb{Z}_n, (a,n)=1}^{n-1} |Fix(a)|$$

Ora ragioniamo un momento sugli elementi fissati da a, vale che $ax \equiv_n x \Leftrightarrow (a-1)x \equiv_n 0$ In generale una equazione $kx \equiv_h 0$ ha una unica soluzione se $(k, h) = 1$, quindi possiamo dire che l'equazione è equivalente a dire:

$$(a-1)x \equiv_n 0 \Leftrightarrow \frac{(a-1)}{(a-1,n)}x \equiv_{\frac{n}{(a-1,n)}} 0$$

L'ultima ha una unica soluzione in $\mathbb{Z}_{\frac{n}{(a-1,n)}}$ e quindi la precedente ne ha $(a-1, n)$ in $\mathbb{Z}_n$. Perciò $|Fix(a)| = (a-1, n)$ da cui si conclude la dimostrazione.

Soluzione 8.3. Chiamiamo G il gruppo delle rotazioni del tetraedro e consideriamo i 4 spigoli del tetraedro. Ogni rotazione del tetraedro manda questi 4 punti in se stessi, quindi possiamo creare una applicazione $f : G \to S_4$ che manda ogni rotazione $g \in G$ nella permutazione che rappresenta come g scambia gli spigoli. Tale f è chiaramente un morfismo iniettivo visto che una rotazione che fissa i 4 spigoli deve necessariamente fissare tutto il tetraedro ed è pertanto l'identità. Quindi G è isomorfo ad un sottogruppo di S_4. Infine fissati due vertici adiacenti una rotazione può mandare il primo vertice in tutti gli altri 4, il secondo vertice negli altri 3 ed in quel momento i vertici di arrivo degli altri due saranno fissati, in totale ci sono 12 rotazioni possibili. Poiché l'unico sottogruppo con 12 elementi di S_4 è A_4 la tesi è dimostrata.

Soluzione 8.4. Ancora una volta chiamando G il gruppo delle rotazioni del cubo e consideriamo le 4 diagonali maggiori del cubo. Similmente a prima ogni rotazione del cubo manda le diagonali in se stesse, quindi possiamo creare ancora una volta una applicazione $f : G \to S_4$. Tale f è chiaramente un morfismo, ma stavolta non è così istantaneo mostrare che sia iniettivo. A tal proposito se una rotazione tenesse fisse le diagonali vorrebbe dire che ogni spigolo andrebbe nel suo opposto o rimarrebbe fisso. Se siffatta rotazione mandasse uno spigolo nel suo opposto e fissasse le diagonali risulta immediato vedere che dovrebbe mandare ogni spigolo nel proprio opposto per mantenere le relazioni di adiacenza fra spigoli, quindi agirebbe come l'applicazione lineare $-Id$ che, avendo determinante, -1 non potrebbe rappresentare una rotazione. Da qui si deduce che l'unica rotazione che fissa le diagonali è l'identità, pertanto il morfismo f è iniettivo. Infine una rotazione del cubo può portare un primo spigolo in uno qualsiasi degli 8 spigoli ed un secondo

spigolo adiacente al primo in uno qualsiasi dei 3 spigoli adiacenti allo spigolo di arrivo del primo. Ma una volta fissate queste due scelte tutti gli altri spigoli hanno destinazioni fissate. Quindi in totale ci sono G ha $8 \cdot 3 = 24$ elementi, tanti quanti S_4! Da cui la tesi è dimostrata.

Soluzione 8.5. 1. Risulta essere una azione poiché:

$$[(P_1, Q_1) \times (P_2, Q_2)] * A = (P_1P_2, Q_1Q_2) * A = P_1P_2AQ_2^{-1}Q_1^{-1} = (P_1, Q_1) * [(P_2, Q_2) * A]$$

2. Occorre notare che questa azione corrisponde allo scrivere la matrice A rispetto a due basi diverse, infatti se vedessimo A come applicazione lineare da $\mathbb{R}^n$ a $\mathbb{R}^m$ allora varrebbe che:

$$Av = P^{-1}PAQ^{-1}Qv = PAQ^{-1}w$$

Dove w è scritto usando una base differente con matrice di cambio di base Q ed il vettore di arrivo è scritto usando una base differente con cambio di base P^{-1}. In più risulta immediato osservare che l'azione sopra mantiene inalterato il rango della matrice. Inoltre tutte le matrici con lo stesso rango sono nella stessa orbita visto che presa una base del $ker(A), \{v_1, v_2, \cdots, v_j\}$ e completandola ad una base di tutto $\mathbb{R}^n, \{v_{j+1}, \cdots, v_n\}$, allora usando come base di $\mathbb{R}^m$ la base: $\{Av_{j+1}, \cdots, Av_n\}$ eventualmente completata ad una base di tutto $\mathbb{R}^m$ si ha che A in questa base si scrive come:

$$\begin{pmatrix} 0 & Id \\ 0 & 0 \end{pmatrix}$$

Dove lo "spessore" della parte non nulla dipende solamente dal $ker(A) = n - rk(A)$. Questo vuol dire che l'azione ha solamente n orbite, una per ogni possibile rango di A.

3. Se scrivessimo la matrice Q a blocchi di opportune dimensioni otterremmo:

$$\begin{pmatrix} Id & 0 \end{pmatrix} = P \begin{pmatrix} Id & 0 \end{pmatrix} \begin{pmatrix} Q_{1,1} & Q_{1,2} \\ Q_{2,1} & Q_{2,2} \end{pmatrix} \Leftrightarrow \begin{cases} PQ_{1,1} = Id \\ PQ_{1,2} = 0 \end{cases} \Leftrightarrow \begin{cases} Q_{1,1} = P^{-1} \\ Q_{1,2} = 0 \end{cases}$$

Da cui si ottiene che lo stabilizzatore di quella matrice sono le coppie del tipo:

$$\left(P, \begin{pmatrix} P^{-1} & 0 \\ A & B \end{pmatrix}\right)$$

con $B \in GL_{n-m}(\mathbb{R})$.

Soluzione 8.6. Il coniugio, similmente a sopra, rappresenta il cambio di base, stavolta però considerando una stessa base sia nello spazio di partenza che nello spazio di arrivo (infatti in questo caso coincidono!). Risulta chiaro perciò che l'orbita di quella matrice siano tutte le matrici diagonalizzabili aventi $\{1, 2\}$ come autovalori. Per quanto riguarda lo stabilizzatore, notiamo che una matrice stabilizza quella data se e solo commutano fra di loro, perciò il controllo è immediato:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Leftrightarrow b = c = 0$$

Da cui lo stabilizzatore consiste nelle matrici del tipo: $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ con $a, d \neq 0$. Nulla cambia nel caso il campo base cambiasse.

9 Soluzioni foglio 9

Soluzione 9.1. Applicando i teoremi di Sylow notiamo che devono valere le relazioni:

$$\begin{cases} n_3 | 2 \\ n_3 \equiv_3 1 \\ n_2 | 9 \\ n_2 \equiv_2 1 \end{cases}$$

Da cui $n_3 = 1$ mentre n_2 può essere 1,3 oppure 9. Osserviamo che il 3-Sylow può essere $\mathbb{Z}_9$ o $\mathbb{Z}_3 \times \mathbb{Z}_3$ ed è sempre normale, mentre il 2-Sylow può essere solo $\mathbb{Z}_2$, poiché il loro prodotto è G osserviamo che G si può sempre scrivere come prodotto semidiretto dei due, da cui si hanno le possibilità: $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_9, \mathbb{Z}_2 \ltimes (\mathbb{Z}_3 \times \mathbb{Z}_3), \mathbb{Z}_2 \ltimes \mathbb{Z}_9$. Per l'ultimo prodotto semidiretto Osserviamo che c'è solo un morfismo non banale $\mathbb{Z}_2 \to \mathbb{Z}_9^*$ che inverte tutti gli elementi di $\mathbb{Z}_9$, questo ci porta al gruppo diedrale D_9. Con una dose non banale di intuito e conti è possibile far vedere che i tanti prodotti semidiretti del penultimo caso portano tutti a due possibili gruppi: il primo è dato dal morfismo $\mathbb{Z}_2 \to Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$ che inverte ogni elemento e crea un gruppo che scritto per generatori e relazioni risulta essere: $G = \langle x, y, z | x^3 = y^3 = z^2 = id, xy = yx, xz = zx^2, yz = zy^2 \rangle$. Il secondo è dato dal morfismo $\mathbb{Z}_2 \to Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$ che scambia i due generatori e crea un gruppo che scritto per generatori e relazioni risulta essere: $G = \langle x, y, z | x^3 = y^3 = z^2 = id, xy = yx, xz = zy \rangle$.

Soluzione 9.2. Se i 3−Sylow non fossero normali ve ne dovrebbero essere esattamente 4, presi due di questi 3−Sylow e supponendo per assurdo che non si intersechino, componendo i nove elementi del primo gruppo con i nove dell'altro potrei creare 81 elementi diversi, cosa assurda! Quindi devono intersecarsi in un sottogruppo di tre elementi obbligatoriamente.

Soluzione 9.3. Anzitutto bisogna osservare che i 7-Sylow non possono che essere gruppi ciclici generati da una permutazione fra 7 elementi. Di queste permutazioni ve ne stanno $7!/7 = 6!$, e vanno raggruppate in gruppi da 6 per formare un 7-Sylow, quindi in totale abbiamo 5! 7-Sylow. Agendo ora per coniugio su H uno di questi Sylow dobbiamo ottenere tutti gli altri, l'azione per coniugio di S_7 sull'insieme di 5! elementi dei 7-Sylow transitiva e vale che $|G| = |G_H||O_H|$. Ma l'orbita di H è pari a tutti i 7-Sylow, mentre lo stabilizzatore non è altro che il sottogruppo di $G = S_7$ che fissa H per coniugio, ossia il K che stavamo cercando. Perciò si ottiene che $|K| = 7 \cdot 6$.

Soluzione 9.4.

1. Utilizzando i teoremi di Sylow emerge che se la richiesta verrebbe soddisfatta solo se $n_7 = 15, n_5 = 21$, ma in tal caso avremmo $4 \cdot 21 = 84$ elementi sparsi per i 5-Sylow e $6 \cdot 15 = 90$ elementi sparsi per i 7-Sylow, cosa impossibile. Quindi uno dei due deve essere normale.

2. Sapendo che uno dei due è normale varrebbe che $H_7H_5 = H_5H_7$, quindi ci sarebbe un sottogruppo da 35 elementi in G e potremmo scrivere $H_5H_7 = \mathbb{Z}_5 \ltimes \mathbb{Z}_7$ oppure $H_5H_7 = \mathbb{Z}_5 \rtimes \mathbb{Z}_7$. Tuttavia è immediato notare che questi prodotti semidiretti devono obbligatoriamente essere diretti, poiché per questioni di ordine gli automorfismi devono essere banali, quindi $H_5H_7 = \mathbb{Z}_5 \times \mathbb{Z}_7$ ed è immediato osservare che l'elemento $(1, 1)$ ha ordine 35.

Soluzione 9.5.

1. Il terzo teorema di Sylow ci assicura che $n_2 = 1$ o 5. Pensando D_{10} come gruppo di riflessione di un decagono, un 2-Sylow è un sottogruppo di ordine 4, è facile vedere che le riflessioni rispetto a due assi di simmetria perpendicolari del decagono formano un sottogruppo di ordine 4. Questi sono 5 e sono tutti isomorfi al gruppo di Klein. Usando la presentazione $\langle s, t | s^2 = t^10 = e, sts^{-1} = t^{-1}t \rangle$ è facile scriverli:

$$\{id, s, t^5, st^5\}, \{id, st, t^5, st^6\}, \{id, st^2, t^5, st^7\}, \{id, st^3, t^5, st^8\}, \{id, st^4, t^5, st^9\}.$$

2. $T \cong A_4$ per un esercizio precedente, è facile vedere che questo ha solo 4 elementi di ordine una potenza di due: $id, (12)(34), (13)(24), (14)(23)$, e quindi questi formano un sottogruppo di ordine 4, che è l'unico 2-sylow ed è isomorfo al gruppo di Klein. Se lo si vuole guardare con le simmetrie di rotazione del tetraedo: data l'azione di permutazione sull'insieme degli spigoli data da T, è il sottogruppo di trasformazioni che fissa o inverte due spigoli opposti fissati.

3. $T \cong S_4$ Il terzo teorema di Sylow ci assicura che $n_2 = 1$. Il 2-Sylow è quindi il sottogruppo delle permutazioni che sono della forma: $id, (ab), (ab)(cd), (abcd)$ con a, b, c, d i numeri da 1 a 4. Avendo un elemento di ordine 4, è facile vedere che questo gruppo deve essere D_4 (costruendo un isomorfismo esplicito o usando la classificazione dei gruppi di ordine 8). Se consideriamo l'azione di permutazione del gruppo sull'insieme delle diagonali, che è fedele e transitiva per quanto visto in un esercizio precedente, possiamo identificare D_4 con un sottogruppo di simmetrie rotazionali del cubo.

4. Il gruppo di simmetrie rotazionali di un dodecaedro è A_5, per il terzo teorema di sylow $n_2 = 1$ o 3 o 5 o 15. Possiamo trovare 5 immersioni di A_4 in A_5 date nel seguente modo: per ogni i in $\{1,2,3,4,5\}$, possiamo considerare le permutazioni pari dei numeri complementari a i in questo insieme. Ognuna di queste cinque immersioni ci fornisce un sottogruppo isomorfo al 2-Sylow di A_4. Quindi visto che il 2-Sylow di A_4 e quelli di A_5 hanno lo stesso ordine, ho trovato almeno 5 2-Sylow di A_5, tutti chiaramente isomorfi al gruppo di Klein. Sia V_4 il 2-Sylow dato dall'immersione con $i = 5$, se ci fossero 15 2-Sylow avremmo che, per il terzo teorema di Sylow, $|N_{A_5}(V_4)| = 8$, da cui se ne dedurrebbe che $N_{A_5}(V_4) = V_4$: questo non è possibile in quanto, ad esempio, il coniugio per (123) stabilizza V_4.

Soluzione 9.6. Notiamo che un'applicazione lineare invertibile su $\mathbb{F}_p^2$ è univocamente determinata dai vettori di arrivo della base $\{(1,0),(0,1)\}$. Il primo vettore ha p^2-1 vettori di arrivo dovendo escludere il vettore nullo per invertibilità, mentre il secondo ne ha $p^2-1-(p-1)$ visto che bisogna escludere sia il vettore nullo che lo span del primo. In totale quindi vi sono $(p^2-1)(p^2-1-p+1) = p(p-1)^2(p+1)$ elementi in $\mathbb{F}_p^2$ ed un $p-$Sylow avrà perciò soltanto p elementi.

A questo punto la scelta più naturale è il sottogruppo di matrici

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_p \right\} \simeq \mathbb{F}_p$$

dove l'isomorfismo è evidente dal fatto che:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

10 Soluzioni foglio 10

Soluzione 10.1. 1. Sia $P' \subset N$ il $p-$Sylow di N contenente $P \cap N$. Sicuramente questo è contenuto in un $p-$Sylow $P' \subset P''$ di G per cui valga $P'' \cap N = P'$. Ricordiamo però che i $p-$Sylow di G sono tutti coniugati, quindi esiste $g \in G$ per cui $gPg^{-1} = P''$ e quindi $gPg^1 \cap N = P'' \cap N$. Tuttavia per normalità $N = gNg^{-1}$, perciò:

$$P' = P'' \cap N = gPg^1 \cap N = gPg^1 \cap gNg^{-1} = g(P \cap N)g^{-1}$$

Da cui emerge che P' e $P \cap N$ hanno la stessa cardinalità, ma essendo uno un sottogruppo dell'altro devono per forza essere uguali.

2. Sia $P' \subset G/N$ il $p-$Sylow di G/N contenente PN/N. Scrivendo $|G| = p^a \cdot dc$ e $|N| = p^b \cdot d$ sappiamo dal punto precedente che $|P \cap N| = p^b$ in quanto $p-$Sylow di N. Inoltre dal secondo teorema degli isomorfismi (diamante) $NP/N \simeq P/N \cap P$, perciò $|NP/N| = p^{a-b}$. Osservando che $|G/N| = p^{a-b} \cdot c$ è immediato notare che PN/N è un $p-$gruppo di cardinalità massima, perciò è un $p-$Sylow.

Soluzione 10.2. Supponiamo per assurdo che ogni Sylow non sia normale, allora devono valere le seguenti relazioni fra i numeri di Sylow:

$$\begin{cases} n_p | rq \\ n_p \equiv_p 1 \\ n_p \neq 1 \end{cases} \quad \begin{cases} n_q | pr \\ n_q \equiv_q 1 \\ n_q \neq 1 \end{cases} \quad \begin{cases} n_r | pq \\ n_r \equiv_r 1 \\ n_r \neq 1 \end{cases}$$

Poiché avevamo disposto $p < q < r$ abbiamo una sola scelta per $n_r = pq$, per ragioni analoghe la scelta più piccola che possiamo fare per n_q è $n_q = r$. Infine la scelta più piccola per n_p è $n_p = q$. Ogni Sylow pertanto sarà un gruppo ciclico di ordine primo, quindi due Sylow diversi non potranno mai intersecarsi. In totale quindi avremmo $n_p \cdot (p-1)$ elementi di ordine p, $n_q \cdot (q-1)$

elementi di ordine q e $n_r \cdot (r-1)$ elementi di ordine r. In totale quindi gli elementi sarebbero almeno:

$$q(p-1) + r(q-1) + pq(r-1) = pqr + qr - q - r$$

Ma essendo tutti interi positivi $qr - q - r > 0$, quindi avremmo sforato la cardinalità del gruppo ottenendo un assurdo.

Soluzione 10.3. 1. La prima dimostrazione è banale

2. Sia $n \in N_G(H)$, allora per ogni $c \in C_G(H)$ vale che $ncn^{-1} \in C_G(H)$, infatti per ogni $h \in H$ notiamo che:
$$ncn^{-1}h\left(ncn^{-1}\right)^{-1} = h \Leftrightarrow cn^{-1}hnc^{-1} = n^{-1}hn$$
Ma poiché $nhn^{-1} \in H \forall h \in H, n \in N$ e visto che c commuta con tutti gli elementi di H l'uguaglianza sopra è verificata.

3. La scelta più naturale è $N_G(H) \to Aut(H)$ con $n \mapsto \phi_n$ dove $\phi_n(h) = nhn^{-1}$. Questo è un morfismo poiché:
$$\phi_n(\phi_m(h)) = \phi_n(mhm^{-1}) = (nmn^{-1})(nhn^{-1})(nm^{-1}n^{-1}) = nmhm^{-1}n^{-1} = \phi_{nm}(h)$$
Ed il kernel è dato dagli $n \in N$ per cui $\phi_n(h) = h \ \forall h \in H$, ovvero $nhn^{-1} = h \ \forall h \in H$. Perciò il kernel è esattamente $C_G(H)$.

Soluzione 10.4. 1. Consideriamo l'azione del coniugio di G con $|G| = p^n$ su se stesso, secondo questa azione lo stabilizzatore di un elemento è esattamente il suo centralizzatore. Sapendo che il centro contiene esattamente p elementi possiamo notare che G ha esattamente p orbite composte da singoli elementi. Analogamente un elemento ha centralizzatore con cardinalità p^{n-1} se e solo se sta in una orbita con p elementi. Se supponessimo per assurdo che non vi siano orbite con p elementi otterremo che G ha p orbite con un elemento, k_2 orbite con p^2 elementi, k_3 orbite con p^3 elementi e così via. Perciò contando gli elementi orbita per orbita otterremo che gli elementi di G sono:
$$p^n = |G| = p + k_2p^2 + k_3p^3 + \cdots$$
ma passando tutto in congruenza modulo p^2 otterremmo che $0 = p \mod p^2$, assurdo.

2. Consideriamo x con il centralizzatore di cardinalità p^{n-1}, se uno degli elementi del centralizzatore di x avesse ordine maggiore o uguale di p^3 allora lui o una sua potenza genererebbero un sottogruppo ciclico con p^3 elementi, da cui la tesi. Invece se tutti gli elementi del centralizzatpre avessero ordine p potrei sicuramente trovare $y \in C_G(x) \setminus \langle x, Z(G)\rangle$ visto che il gruppo a sinistra contiene almento p^3 elementi mentre quello a destra ne ha p^2, in tal caso posso definire $H = \langle Z(G), x, y\rangle$ che è abeliano di ordine p^3 in quanto generato da elementi di ordine p che commutano fra loro. Rimane da considerare il caso in cui gli elementi del centralizzatore abbiano ordine p^2 o p. Qualora x avesse ordine p^2 e potessi prendere $y \in C_G(x) \setminus \langle x\rangle$ di ordine p concludo ponendo $H = \langle x, y\rangle$ che è un gruppo abeliano di ordine p^3. Infine se qualsiasi y avesse ordine p^2 saprei che y^p sarebbe in $\langle x\rangle$ avendo ordine p ed in questo caso $H = \langle x, y\rangle$ sarebbe abeliano di ordine p^3 visto che dal secondo teorema degli isomorfismi:
$$\frac{|\langle x, y\rangle|}{|\langle x\rangle|} = \frac{|\langle y\rangle|}{|\langle x\rangle \cap \langle y\rangle|} \Leftrightarrow |\langle x, y\rangle| = \frac{|\langle x\rangle||\langle y\rangle|}{|\langle x\rangle \cap \langle y\rangle|} = \frac{p^2p^2}{p}$$

Soluzione 10.5. Se G è un gruppo abeliano con p^3 elementi consideriamo l'ordine massimo degli un elementi che compaiono nel gruppo:

1. Nel caso esista un elemento di ordine p^3, G sarebbe ciclico di ordine p^3, isomorfo a C_{p^3}.

2. Se esistesse un elemento g di ordine p^2 allora ci sarebbe un sottogruppo isomorfo a C_{p^2} e potremmo scrivere la successione esatta corta:

$$0 \to C_{p^2} \to G \to C_p \to 0$$

se per assurdo non si spezzasse, ovvero se non esistesse alcun elemento di ordine p al di fuori di C_{p^2} allora varrebbe che tutti gli elementi h fuori da C_{p^2} avrebbero ordine p^2 (se fosse p^3 torneremo al caso sopra), in particolare varrebbe che $h^p \in \langle g^p \rangle$, quindi per qualche m varrebbe che $h^p = g^{pm}$, da cui otterremo un assurdo visto che l'elemento hg^{-m} non è in C_{p^2} ma ha ordine p. In conclusione la successione si spezza sempre quindi $G = C_P \times C_{p^2}$.

3. Se ogni elemento avesse ordine p esisterebbero sicuramente tre elementi x, y, z i cui span non possono intersecarsi per cui $G = \langle x \rangle \times \langle y \rangle \times \langle z \rangle = (C_p)^3$.

Soluzione 10.6. Se $x^n = 0$ allora:

$$(1+x)(1-x+x^2-x^3 \cdots (-1)^n x^n = 1 + x - x + x^2 - x^2 \cdots (-1)^n x^n (-1)^n x^{n+1} = 1$$

$$(1-x)(1+x+x^2+x^3 \cdots + x^n = 1 + x - x + x^2 - x^2 \cdots + x^n - x^{n+1} = 1$$

Soluzione 10.7. Anzitutto dobbiamo osservare che in un anello Booleano $a + a = 0 \ \forall a \in R$, infatti

$$a + a = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a \Rightarrow a + a = 0$$

quindi $a = -a$. Ciò detto per ogni $x, y \in R$ vale che:

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx \Rightarrow xy = -yx \Rightarrow xy = -yx$$

Soluzione 10.8.

1. Se l'anello è commutativo allora presi $x, y \in Nil(R)$ con $x^n = y^m = 0$ vale che:

$$(x+y)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} x^j y^{n+m-j}$$

E quegli addendi sono tutti nulli visto che per $j \geq n$ le potenze di x si annullano mentre per gli altri j si annullano quelle di y. Invece presi $x \in Nil(R)$ ed $y \in R$ con $x^n = 0$ vale che $(xy)^n = x^n y^n = 0$, da cui otteniamo la tesi.

2. Come controesempio prendiamo $R = M_{2,2}(\mathbb{R})$, allora $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in Nil(R)$ ma

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin Nil(R).$$

11 Soluzioni foglio 11

Di seguito trovate una traccia delle soluzioni, che includono le idee necessarie per svolgere gli esercizi.

Soluzione 11.1. 1. Se $I+J+K=A$, allora posso scrivere $1=a+b+c$ con $a\in I, b\in J, c\in K$. di conseguenza si ha che $(a+b+c)^{3n}=1$, sviluppando si trovano tre elementi voluti che sommano a 1.

2. Se $J+K=A$, allora $IJ+JK+KI=I(J+K)+KJ=I+KJ$. Inoltre $I+K=I+J=A$ ci dice che esistono i,j e i',k tali che $1=i+j$ e $1=i'+k$. Da questo si ha che $1=(i+j)(i'+k)\in I+KJ$, da cui la tesi.

Soluzione 11.2. 1. In generale, se A ufd e $I=(a)$, $J=(b)$ con a e b coprimi, allora $IJ=I\cap J=(ab)$. Inoltre se A è anche dominio euclideo, vale $(a)+(b)=A$ (basta dominio di Bezout in realtà). Nel nostro caso (dopo le opportune verifiche) abbiamo quindi che $IJ=I\cap J=((x^2+1)(x^3-1))$. Inoltre $I+J=A$ in quanto i due polinomi sono coprimi.

2. $-(x-1)(y-1)+(x-1)+(y-1)=xy-1$, dunque $J\subset I$. $Q[x,y]/I$ è un campo, infatti la mappa suriettiva

$$\begin{aligned}\mathbb{Q}[x,y]&\to\mathbb{Q}\\ x&\mapsto 1\\ y&\mapsto 1\end{aligned}$$

ha kernel I. Inoltre $x+1\notin J$, quindi J non può essere massimale. J è però primo, in quanto $\mathbb{Q}[x,y]$ è un anello a fattorizzazione unica e $xy-1$ è irriducibile.

3. a) Usando l'esercizio 10.8: consideriamo la mappa quoziente $A\to A/I$, per il teorema di corrispondenza fra ideali $Nil(A/I)$ corrisponde ad un ideale in A, e per definizione questo è proprio $\sqrt{I}$.
   b) È facile vedere che $\sqrt{IJ}\subset\sqrt{I\cap J}\subset\sqrt{I}\cap\sqrt{J}$. Infine $\sqrt{I}\cap\sqrt{J}\subset\sqrt{IJ}$ perché se $x^n\in I$ e $x^m\in J$, allora $x^{n+m}\in IJ$.
   c) Basta osservare che $(x^n)^m=x^{nm}\in I$.

Soluzione 11.3. L'ipotesi ci fornisce un isomorfismo $A/\operatorname{Ker}\phi\to B$.Visto che B è un dominio $\operatorname{Ker}\phi$ è un primo. Ma in un pid, ogni ideale primo non nullo è massimale (vedere esercizio successivo). Dunque se $\ker\phi$ è nullo ϕ è un isomorfismo, altrimenti B è il quoziente per un ideale massimale, dunque un campo.

Soluzione 11.4. Per assurdo: supponiamo di avere $(a)\subsetneq(b)\subsetneq A$ ideali primi. Allora $a=bk$ con $k\in A$, da cui necessariamente $k=aj$ con $j\in A$ perché (a) è primo. Abbiamo quindi che $a=baj$ e dunque $1=bj$, che è assurdo in quanto (b) è un ideale proprio.

Soluzione 11.5.
- Falso. Basta prendere $A\subset B$ con A dominio e B non dominio. E considerare $P=(0)$. Ad esempio la proiezione $\mathbb{Z}\to\mathbb{Z}/6\mathbb{Z}$.
- Falso. Controesempio dato da $\mathbb{Q}\subset\mathbb{Q}[x]$ e l'unico ideale proprio di $\mathbb{Q}$.
- Vero. Infatti se $ab\in f^{-1}(P)$, allora $f(a)f(b)\in P$ e, senza perdita di generalità, $f(a)\in P$. Da cui $a\in f^{-1}(P)$.
- Falso. Basta considerare $\mathbb{Z}\subset\mathbb{Q}$ e $M=0$.

12 Soluzioni foglio 12

Soluzione 12.1. Notiamo immediatamente che il suggerimento $A \to A/I^2$ dove $x \mapsto \overline{xp}$ e $I = (p)$ contiene già il primo isomorfismo richiesto, infatti in questo morfismo moltiplichiamo ogni elemento per il generatore dell'ideale, perciò l'immagine è contenuta nell'ideale generato da p, inoltre essendo l'anello unitario la classe di $1 \cdot p$ è nell'immagine, quindi l'immagine è esattamente I/I^2. Per quanto riguarda il Kernel è chiaro che l'ideale generato da p verrebbe moltiplicato per p e finirebbe dentro (p^2), ovvero in zero. Viceversa preso $x \in A$ con $xp \in (p^2)$ varrebbe che per qualche $y \in A$ $xp = yp^2$ ma per le leggi di cancellazione vorrebbe dire che $x = yp$, perciò $x \in (p)$. In conclusione l'immagine del morfismo sopra è $(p)/(p^2)$ mentre il kernel è (p) e dal teorema sugli isomorfismi quindi: $A/(p) \simeq (p)/(p^2)$.

In realtà possiamo generalizzare il procedimento usando il morfismo $A \to A/(p^{k+1})$, $x \mapsto \overline{xp^k}$ che con procedimento analogo ha kernel (p) ed immagine (p^k) per ottenere un isomorfismo $A/(p) \simeq (p^k)/(p^{k+1})$.

Usando l'ultimo suggerimento notiamo che:

$$A/(p^k) \simeq \frac{A/(p^{k+1})}{(p^k)/(p^{k+1})} \simeq \frac{A/(p^{k+1})}{A/(p)} \Rightarrow |A/(p^{k+1})| = |A/(p^k)||A/(p)|$$

E da questa equazione induttiva si ottiene la tesi.

Soluzione 12.2. Iniziamo osservando che preso un polinomio $p(x)$ dire che $p(a) = b$ equivale a dire che $p(a) - b = 0$, ovvero che $q(x) = p(x) - b$ ha come divisore $(x - a)$, quindi che $p(x)$ è congruo a b modulo $(x - a)$. In altre parole occorre risolvere il sistema di equazioni modulari:

$$\begin{cases} p(x) \equiv b_1 & \mod x - a_1 \\ p(x) \equiv b_2 & \mod x - a_2 \\ \vdots & \\ p(x) \equiv b_n & \mod x - a_n \end{cases}$$

E poiché gli ideali $(x-a_i), (x-a_j)$ sono a due a due coprimi esiste una unica soluzione modulo $q(x) = \left(\prod_{j=1}^{n}(x - a_j)\right)$. Quindi sia $p(x)$ una soluzione del genere, eseguendo una divisione euclidea $p(x) = q(x) \cdot m(x) + r(x)$ si ottiene il polinomio cercato $r(x)$ di grado al più $n - 1$. Infine notiamo che se esistessero due polinomi con le proprietà richieste $p(x), q(x)$ allora la differenza sarebbe un polinomio di grado al più $n - 1$ che si annullerebbe in n valori distinti, cosa possibile solo per il polinomio nullo. Quindi i due devono essere uguali.

Soluzione 12.3. Usando i diversi teoremi sugli isomorfismi otteniamo la catena di isomorfismi:

$$\mathbb{Q}[x,y]/(x-y, x^3+y^3-x) \equiv \frac{\mathbb{Q}[x,y]/(x-y)}{(x-y, x^3+y^3-x)/(x-y)} \equiv \mathbb{Q}[x]/(2x^3-x) \equiv \mathbb{Q}[x]/(x\cdot(2x^2-1)) \equiv$$

$$\mathbb{Q}[x]/(x) \times \mathbb{Q}[x]/(2x^2-1) \equiv \mathbb{Q} \times \mathbb{Q}[1/\sqrt{2}]$$

Dove nel penultimo passaggio si è usato che gli ideali $(x), (2x^2 + 1)$ sono coprimi. Questa è una perfetta descrizione dell'anello come prodotto di campi da cui risulta ovvio che il modulo è uno spazio vettoriale di dimensione 3.

Soluzione 12.4. 1. Iniziamo osservando che $\mathbb{Z}[x]/(x^2+1) \equiv \mathbb{Z}[i]$ e proseguiamo ricordando che ogni morfismo fra anelli unitari deve portare l'unità nell'unità e questo fissa tutto il suo span algebrico, ovvero i numeri interi. Ora poiché in $\mathbb{Z}[i]$ vale la relazione $i \cdot i = 1$, l'immagine di i deve essere un elemento di $\mathbb{C}$ che moltiplicato a se stesso dia 1, ma gli elementi del genere sono solo $\pm i$. Quindi i due possibili morfismi sono l'immersione canonica e la coniugazione complessa. Entrambi iniettivi.

2. Notiamo che preso un morfismo $F : \mathbb{Z}[x]/(p(x)) \to \mathbb{R}$ sia $\alpha = F(x)$. Allora visto che il morfismo deve mandare l'unità nell'unità e fissa quindi tutti i numeri interi deve valere che per ogni polinomio $F(p(x)) = p(\alpha)$. Ma se $(p(x))$ è nel kernel deve necessariamente valere che $p(\alpha) = 0$. Quindi affinché possa esistere un morfismo unitario il polinomio deve possedere almeno una radice reale in cui mandare x. Infine il morfismo è iniettivo se e solo se per ogni polinomio $q(x)$ con $q(\alpha) = 0$ vale che q è multiplo di p, ovvero $p(x)$ deve essere a meno di multipli interi il polinomio di grado minimo che si annulla in α.

Soluzione 12.5. Sappiamo che $A \equiv A[x]/(x)$, quindi per mostrare che è un campo basta mostrare che (x) è un ideale massimale. Tuttavia essendo in un PID ogni ideale è massimale se e solo se è generato da un elemento irriducibile. Tuttavia se potessimo scrivere x come un prodotto di polinomio è chiaro osservare che uno dovrebbe avere grado zero e l'altro grado uno. Da cui $x = a_1 \cdot (a_2 x + a_3)$. Quindi deve valere in particolare che $a_1 \cdot a_2 = 1$, ovvero a_1 è invertibile, da cui l'irriducibilità di x e la tesi.

Soluzione 12.6. Iniziamo osservando che un ideale massimale M di $\mathbb{Z}[x]$ deve necessariamente contenere dei numeri interi anche detti polinomi di grado nullo, in caso contrario $\mathbb{Z}[x]/M$ sarebbe un campo e quindi potrei invertire anche i polinomi di grado zero. Tuttavia questo equivale a chiedere che preso $m \in \mathbb{Z}$ dovrebbe valere che $m - 1 \in M$ ovvero che $m - 1$ è multiplo di un qualche polinomio, cosa assurda.

Proseguiamo notando che sia m il più piccolo elemento non nullo intero di M, allora necessariamente deve essere un numero primo poiché se avesse un divisore d potrei creare un ideale più grande (M, d) contraddicendo la massimalità. Otteniamo quindi che esiste sempre un numero primo dentro M e non ve ne possono essere altri altrimenti per identità di Bezout ci sarebbe anche l'unità contraddicendo la massimalità.

Usando il terzo teorema degli isomorfismisappiamo che

$$\mathbb{Z}[x]/M \simeq \frac{Z[x]/(p)}{M/(p)} \simeq \frac{\mathbb{Z}_p[x]}{M/(p)}$$

Ma $\mathbb{Z}_p$ è un campo, quindi $Z_p[x]$ è un dominio ad ideali principali, ed essendo $M/(p)$ massimali sappiamo che deve essere generato da un irriducibile dentro $\mathbb{Z}_p[x]$. Quindi esiste un polinomio irriducibile $q(x)$ modulo p con $M/(p) = (q(x))$.

Quindi è immediato osservare che gli ideali massimali di $\mathbb{Z}[x]$ sono tutti e soli gli ideali del tipo $(p, q(x))$ con p intero primo e $q(x)$ irriducibile in $Z_p[x]$.

13 Soluzioni foglio 13

Soluzione 13.1.

1. Osserviamo immediatamente che $(a + ib) \cdot (a - ib) = (a^2 + b^2)$, perciò per poter usare il teorema cinese dei resti bisogna dimostrare che $I = (a + ib) + (a - ib) = \mathbb{Z}[i]$ e che $(a + ib) \cap (a - ib) = (a^2 + b^2)$ per concludere la tesi. Sommando e sottraendo i generatori è chiaro che possiamo ottenere $2a, 2b \in I$ e poichè a, b erano comprimi fra loro possiamo costruire tutti i numeri pari con loro combinazioni intere. Inoltre essendo coprimi uno di loro deve essere pari e l'altro dispari, quindi $a^2 + b^2$ è sempre un numero dispari. Quindi potendo costruire tutti i pari ed un dispari è immediato osservare che possiamo costruire anche l'unità, da cui $1 \in I$. Invece essendo in un dominio ad ideali principali vale che $(a + ib) \cap (a - ib) = (mcm(a + ib, a - ib)), (a + ib, a - ib) = (MCD(a + ib, a - ib)$ e poiché il secondo è tutto l'anello i due elementi sono coprimi e quindi il minimo comune multiplo è il prodotto fra i due, da cui la tesi.

2. Per far funzionare le cose in questo nuovo inseme ci sono diverse soluzioni che si possono tentare, quella che preferisco sta nel mostrare che $B = S^{-1}A$ è ancora un dominio ad ideali principali. Infatti ogni ideale J di B è della forma $S^{-1}I$ dove I è un ideale di A poiché è immediato notare $I = J \cap A$ è un ideale di A e che ogni elemento $j \in J$ è della forma $j = s^{-1}a$ da cui $sj = a$ da cui $a \in J \cap A = I$, quindi $J = S^{-1}I$. Infine essendo gli ideali

di A principali si può trovare un generatore per I e quindi si ripercorrono i passi del punto precedente in cui avevamo usato che l'anello era un dominio ad ideali principali.

Soluzione 13.2. 1. Ovviamente i polinomi del tipo ax^n con a nilpotente sono nilpotenti e poiché la somma di elementi nilpotenti si ha che se tutti i coefficienti sono nilpotenti allora lo è anche il poinomio. Viceversa se per assurdo potesse esserci un polinomio $p(x) = n_0 + n_1 x + \cdots + n_m x^m$ nilpotente con qualche coefficiente n_j non nilpotente allora preso n_l il coefficiente non nilpotente di grado più piccolo potrei sottrarre il polinomio $q(x) = n_0 + \cdots + n_{l-1}x^{l-1}$ ed avere che $p(x) - q(x) = n_l x^l + \cdots + n_m x^m$ è ancora nilpotente, cosa assurda perché il termine di grado minore è dato da potenze di n_l che non è nilpotente.

2. Sia $G(x)$ il polinomio non nullo di grado più piccolo possibile m con coefficiente direttore $g_m \neq 0$ tale che $G(x)F(x) = 0$. Consideriamo adesso il coefficiente f_j di F di grado più alto tale che $f_j G(x) \neq 0$. Abbiamo due opzioni:

   Se tale elemento non esistesse allora ogni coefficiente f_l di F è tale che $f_l G(x) = 0$, ovvero per ogni coppia di coefficienti vale che $f_l g_j = 0$, da cui il polinomio costante non nullo g_m è tale che $g_m F(x) = 0$, cosa possibile se eravamo partiti con un polinomio di grado nullo in partenza.

   Invece se tale elemento esistesse possiamo dedurre che $F(x)G(x) = (f_0 + \cdots + f_j x^j)(g_0 + \cdots + g_m x^m) = 0$, da cui $f_j g_m = 0$ e quindi il polinomio $f_j G(x)$ ha grado più piccolo di $G(x)$ ma rispetta la relazione $F(x) f_j G(x) = 0$, contraddicendo la minimalità.

Soluzione 13.3. 1. Siano $f(x), g(x)$ due polinomi tali che il prodotto abbia tutti i coefficienti in P ideale primo di A. Siano per assurdo f_j, g_l i coefficienti di grado più piccolo in entrambi i polinomi non in P. Allora il termine di grado $j + l$ ha come coefficiente in P:

$$(fg)_{j+l} = \sum_{i=0}^{j+l} f_i g_{j+l-i} = f_0 g_{j+l} + \cdots f_{j-1} g_{l+1} + f_j g_l + f_{j+1} g_{l-1} + \cdots + f_{j+l} g_0.$$

   Quelli a sinistra sono tutti elementi in P perché prima di f_j tutti i coefficienti di f erano in P per ipotesi, analogamente tutti quelli a sinistra sono in P poiché prima di g_l tutti i coefficienti di g erano in P. Quindi in conclusione $f_j g_l \in P$ da cui si ottiene l'assurdo poiché essendo P primo almeno uno di loro deve essere in P.

2. La prima osservazione banale è che il termine noto deve sempre essere invertibile, altrimenti è chiaro che il polinomio non può invertirsi. Purtroppo a parte questo dobbiamo ammettere che c'è un errore di scrittura, infatti la tesi è falsa in un anello non commutativo. Ad esempio usando l'anello delle matrici 2×2 possiamo definire il polinomio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x$$

   Che è composta da un invertibile termine noto più un nilpotente termine di primo grado. Tuttavia se fosse invertibile dovrebbe essere invertibile anche il suo quadrato che con semplici conti risulta essere:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x$$

   che non ha un coefficiente nilpotente di primo grado ed è palesemente non invertibile. La questione sottile è che abbiamo bisogno di una proprietà vera solo in anelli commutativi per garantire questo risultato, ovvero necessitiamo che gli elementi nilpotenti formino un ideale. Se valesse questa proprietà allora tutti gli elementi del tipo $i - n$ con i invertibile ed n nilpotente sarebbero invertibili, infatti $i - n = \left(1 - ni^{-1}\right) i$ da cui ni^{-1} sarebbe ancora nilpotente tale che $\left(ni^{-1}\right)^m = 0$ e quindi possiamo trovare un inverso esplicito in serie di geometrica:

$$(i - n) \cdot \left[i^{-1} \sum_{j=0}^{m-1} \left(ni^{-1}\right)^j \right] = \left(1 - ni^{-1}\right) \left[\sum_{j=0}^{m-1} \left(ni^{-1}\right)^j \right] = 1 - \left(ni^{-1}\right)^m = 1$$

E se la somma di nilpotenti è nilpotente otteniamo che tutti i polinomi di quella forma devono essere invertibili.

Per il viceversa è molto comodo usare un risultato intermedio. Ovvero che gli elementi nilpotenti sono quelli nell'intersezione di tutti gli ideali primi dell'anello. Ovvero:

$$Nil(A) = \bigcap_{P \text{ primo } \subset A} P$$

Infatti se $a^n = 0$ poiché lo zero è contenuto in ogni ideale primo si ottiene che a è un elemento di ogni ideale primo. Viceversa se esistesse un ideale primo con $a \notin P$ allora nessuna potenza di a potrebbe essere in P ed in particolare nessuna potenza di a potrebbe annullarsi.

Usando questo risultato intermedio è chiaro che per ogni ideale primo $P \subset A$ dall'esercizio precedente $A/P[x] = A[x]/P[x]$ è un dominio di integrità, quindi un polinomio $p(x) = a_0 + \cdots + a_n x^n$ è invertibile solo se ogni coefficiente a parte a_0 è nell'ideale primo P, valendo per ogni ideale primo si ha che tutti i coefficienti tranne a_0 sono in tutti gli ideali primi e quindi sono nilpotenti.

Soluzione 13.4. Se i due polinomi p, q fossero coprimi in $\mathbb{Q}[x]$ varrebbe che $1 \in (p, q)$, ovvero ci sarebbero due polinomi h, k a coefficienti razionali con $h(x)p(x) + k(x)q(x) = 1$. Ma se m è il minimo comune multiplo fra tutti i denominatori dei coefficienti di h e k varrebbe che $mh(x)p(x) + mk(x)q(x) = m$ dove tutti i polinomi ora hanno coefficienti interi, quindi nell'anello $\mathbb{Z}[x]$ otteniamo che $m \in (p, q)$. Per il viceversa se $m \in (p, q)_{\mathbb{Z}}$ essendo m invertibile in $\mathbb{Q}$ si ottiene che $1 \in (p, q)_{\mathbb{Q}}$.

Soluzione 13.5.

1. Usando il criterio di Eisenstein con $p = 3$ è immediato notare che è irriducibile.
2. Ancora una volta basta usare il criterio di Eisenstein con $p = 3$.
3. Avendo grado tre ed essendo i coefficienti coprimi è riducibile se e solo se esiste una radice intera, ma tale radice intera deve dividere il termine noto 1 ed è immediato osservare che ± 1 non sono soluzioni.
4. Analogo a sopra, con la differenza che il termine noto è 7 ma ne ± 7, ne ± 1 sono soluzioni.
5. Ancora il criterio di Eisenstein con $p = 3$.

14 Soluzioni foglio 14

Soluzione 14.1.

1. Osserviamo che un polinomio razionale di grado 3 riducibile deve ammettere sempre una radice. Questo però per il teorema delle radici razionali potrebbe avere solo radici $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$ e nessuna di queste annulla il polinomio. Quindi il polinomio è irriducibile in $\mathbb{Q}$ e, poiché i coefficienti non hanno fattori in comune, è irriducibile anche in $\mathbb{Z}$.
2. Osserviamo subito che il polinomio si può scrivere come $7(x^5 - 3x^4 + 15)$, quindi è riducibile in $\mathbb{Z}$. La domanda è: il polinomio "monicizzato" è riducibile in $\mathbb{Q}$? Osserviamo applicando il criterio di Eisenstein con $p = 3$ che è irriducibile negli interi e quindi essendo monico ed irriducibile fra gli interi deve essere anche irriducibile in $\mathbb{Q}$.
3. $x^4 - 5x^2 + 6 = (x^2 - 3)(x^2 - 2)$, completamente riducibile.
4. Applicando il criterio di Eisenstein con $p = 5$ otteniamo che è irriducibile in $\mathbb{Z}$, ma dal lemma di Gauss deve essere irriducibile in $\mathbb{Q}$.

5. Per far vedere che questo è irriducibile la strada conviene spostarci in $\mathbb{F}_2$. otteniamo quindi il polinomio x^5+x^2+1. Immediatamente notiamo che non ha radici in qual campo, quindi potrebbe essere riducibile solo se si spezzasse in un polinomio di grado due (irriducibile) per uno di grado tre. Fortunatamente c'è un solo polinomio irriducibile di grado due in quel campo che è x^2+x+1 e facendo la divisione euclidea fra polinomi si ottiene che:

$$x^5+x^2+1=(x^2+x+1)(x^3+x^2)+1$$

Da cui il polinomio è irriducibile in $\mathbb{F}_2$ e quindi lo è anche in $\mathbb{Z}$ e quindi anche in $\mathbb{Q}$.

Soluzione 14.2. 1. In $\mathbb{F}_2$ il polinomio è già irriducibile in quanto avendo grado 3 e non avendo radici non può scomporsi.

2. In $\mathbb{F}_3$ il polinomio ha come radice 1, da cui si scompone come $(x-1)(x^2+x-1)$ ed il secondo pezzo è irriducibile perché non ha radici.

3. In $\mathbb{F}_5$ il polinomio è ancora irriducibile visto che non ha radici ed ha grado 3.

Soluzione 14.3. 1. Le radici di quel polinomio sono $\pm\frac{\sqrt{2}}{2}\pm i\frac{\sqrt{2}}{2}$. Quindi la scomposizione nei complessi è:

$$x^4+1=(x-(1+i)/\sqrt{2})(x-(1-i)/\sqrt{2})(x+(1+i)/\sqrt{2})(x+(1-i)/\sqrt{2})$$

Quella nei reali è:

$$x^4+1=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$$

Da cui risulta chiaro che il polinomio è irriducibile nei razionali.

2. Essndo in un campo a caratteristica due vale che:

$$x^4+1=(x+1)^4$$

3. La richiesta è equivalente a mostrare che il kernel ha due elementi, cosa ovvia perché esso è composto dagli x con $x^2=1$ che in un campo $\mathbb{F}_2$ sono le radici del polinomio x^2-1 e se $p\neq 2$ sono esattamente i due valori ± 1. In quanto sottogruppo di indice due il prodotto di due elementi al di fuori cascherà sempre lì dentro, visto che il quoziente ha due elementi.

4. L'identità è ovvia, se esistesse un elemento a che al quadrato da -1 allora posso scrivere:

$$x^4+1=x^4-(-1)=(x^2+a)(x^2-a)$$

5. L'dentità è banale, se stavolta valesse che $a^2=2$ allora:

$$x^4+1=(x^2+1)^2-2x^2=(x^2+ax+1)(x^2-ax+1)$$

6. Infine se valesse che $a^2=-2$ allora:

$$x^4+1=(x^2-1)^2-(-2x^2)=(x^2+ax-1)(x^2-ax-1)$$

7. A parte il caso $p=2$ uno fra $-1,2,-2$ ha una radice dentro il campo e posso scomporre il polinomio come sopra.

Soluzione 14.4. Ricordiamo che se un intero di Gauss ha come quadrato della norma un numero primo allora deve necessariamente essere un primo di Gauss.

1. $3+4i$ ha norma 25, quindi dividendolo per un primo con norma 5 come $2+i$ che è primo si ottiene $(2+i)^2=3+4i$.

2. Chiaramente $25=5\cdot 5$ e poiché 5 è congruo ad uno modulo 4 si può scrivere come prodotto di primi di Gauss $5=(2+i)(2-i)$ da cui $25=(2+i)^2(2-i)^2$.

3. Anzitutto $9-15i = 3(3-5i)$ con 3 primo di Gauss in quanto congruo a 3 modulo 4. Invece il secondo ha modulo $9+25 = 34 = 17 \cdot 2$. Quindi dividendolo per un primo di Gauss di norma 2 come $1+i$ si ottiene $3-5i = (1-i)(4-i)$. Il secondo pezzo è un primo a sua volta perché ha norma 17. Da cui: $9-15i = 3(1-i)(4-i)$.

Soluzione 14.5. Un elemento è primo in un anello se e solo se l'ideale che genera è un ideale primo. D'altronde (p) è un ideale primo di $\mathbb{Z}[\sqrt{3}]$ se e solo se $\mathbb{Z}[\sqrt{3}]/(p)$ è un dominio di integrità. Ma:

$$\frac{\mathbb{Z}[\sqrt{3}]}{(p)} \simeq \frac{\mathbb{Z}[x]}{(p, x^2-3)} \simeq \frac{\mathbb{F}_p[x]}{(x^2-3)}$$

Dove l'ultimo è un dominio di integrità se e solo se x^-3 è irriducibile modulo p.

Soluzione 14.6. Essendo l'anello unitario per ogni morfismo di moduli dovrebbe valere:

$$f(m) = f(m \cdot id) = mf(id)$$

Quindi scegliere dove va l'identità basta a caratterizzare il morfismo. Poiché possiamo mandarlo in ogni altro elemento dell'anello vale $Hom(R,R) = R$.

Soluzione 14.7. Dal teorema degli isomorfismi vale che $ker(f) \subset S$, $Imm(f) \subset S'$ sono sottomoduli. Quindi se $Imm(f) = \{0\}$ allora $ker(f) = S$ e si ha il morfismo banale. Oppure se $Imm(f) = S'$ necessariamente $ker(f) = \{0\}$ e si ha un isomorfismo.

15 Soluzioni foglio 15

Soluzione 15.1. Iniziamo ricordando che dato un morfismo $a : \mathbb{Z}^d \to \mathbb{Z}^d$ con associata matrice A che lo rappresenta nella base canonica, vale che l'immagine di a è generata dalle colonne di A, che non sono altro che i vettori di arrivo della base canonica e_j. Ora se trovassimo delle matrici che portano A nella forma canonica di Smith, ovvero se avessimo B, C invertibili intere con $BAC = D$ diagonale allora varrebbe che

$$Imm(A) = Imm(AC) = Imm(B^{-1}D)$$

Visto che l'immagine è generata dalle colonne avremmo che se λ_j sono i termini diagonali di D, l'immagine di A è generata dalle colonne di B ognuna moltiplicata per il suo λ_j.

Ora continuiamo notando che il sottogruppo di $\mathbb{Z}^3$ generato da quei tre vettori corrisponde esattamente all'immagine della matrice che ha quei tre vettori come colonne. Il problema quindi corrisponde a trovare la forma di Smith della matrice:

$$A = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 1 & 1 \\ 3 & 2 & 6 \end{pmatrix}$$

Risulta chiaro che i primi due passaggi sono di sottrarre alla seconda riga la prima e di sottrarre alla terza la prima triplicata, questi corrispondo a moltiplicare a sinistra per la matrice :

$$B = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \Rightarrow \quad BA = \begin{pmatrix} 1 & 3 & 2 \\ 0 & -2 & -1 \\ 0 & -7 & 0 \end{pmatrix}$$

Ora scambiando le ultime due colonne (e cambiando pure i segni) si ottiene una matrice triangolare superiore, questo lo si ottiene moltiplicando a destra per la matrice:

$$C_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad C_1^{-1} = C_1 \Rightarrow BAC_1 = \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 7 \end{pmatrix}$$

Da qui si può procedere operando solo sulle colonne per ridurre tutto alla forma di Smith, non c'è bisogno di trovare la matrice C visto che le operazioni sulle colonne sono ottenute tramite moltiplicazioni a destra ed andranno tutte quante a formare C che a noi non serve. Chiaramente però gli elementi diagonali si manterranno e poiché ci servivano le colonne di B^{-1} moltiplicate per gli elementi diagonali possiamo concludere che desiderata è $(1,1,3)),(0,1,0),(0,0,1)$, che moltiplicata per gli elementi diagonali $1,1,7$ da una base del sottogruppo cercato.

Soluzione 15.2. Risulta ovvio che abbia un insieme di generatori $\{x,y\}$, tuttavia questi generatori non sono linearmente indipendenti poiché la loro combinazione lineare ovvia $(y)x+(-x)y=0$ si annulla. In generale preso un anello R ed un suo sottoanello I questo può ammettere una base visto come R modulo quando è generato da un solo elemento, infatti una qualsiasi coppia di elementi $\{x,y\}$ al suo interno sarà sempre linearmente dipendente per il trucchetto visto prima. Poiché l'ideale di sopra non è generato da un solo elemento, non può ammettere una base.

Soluzione 15.3.

1. La dimostrazione è banale.

2. Consideriamo la base canonica del modulo $\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_4$, $k\in\mathbb{Z}$ è nell'annulatore se e solo se annulla simultaneamente tutti i vettori della base canonica. Ovvero deve valere che:

$$\begin{cases} k\equiv_2 0 \\ k\equiv_3 0 \\ k\equiv_4 0 \end{cases} \Leftrightarrow k\equiv_{12} 0$$

   quindi l'annullatore è (12).

3. Risulta chiaro che l'unico elemento che moltiplicato per ogni intero da zero è zero stesso, da cui l'annullatore è (0).

Soluzione 15.4. Chiaramente nessun elemento di R/I è linearmente indipentende, visto che $I\subset Ann(R/I)$. Quindi ci sono due sole opzioni: $I=(0), I=R$. Nel primo caso il quoziente è l'anello stesso che è un modulo libero generato da 1, nel secondo caso otteniamo il modulo banale (0) che conta come modulo libero.

Soluzione 15.5.

1. Consideriamo $\mathbb{Z}$ come $\mathbb{Z}$ modulo, se prendessimo l'insieme $\{2,3\}$, questi generano tutto $\mathbb{Z}$, tuttavia non formano una base perché sono linearmente dipendenti e $\mathbb{Z}$ non è generato da uno solo dei due, quindi non è possibile estrarre una base.

2. Nello stesso caso di prima consideriamo l'insieme $\{2\}$, questo è linearmente indipendente ma non lo posso estendere ad una base, visto che ogni altro elemento di $\mathbb{Z}$ è linearmente dipendente da 2.

Soluzione 15.6. Utilizziamo la forma di Smith per scrivere la matrice in forma diagonale $BAC=D$, essendo B,C isomorfismo questo vuol dire che esistono due basi di $\mathbb{Z}^k$ in cui A si scrive in forma diagonale. Quindi a meno di ribattezzare $C(\mathbb{Z}^k)=\mathbb{Z}^k$ basta risolvere il problema per A diagonale. In tal caso $\mathbb{Z}^k$ è generato dalla base canonica $\{e_j\}_{j=1,\cdots,k}$ per cui vale $Ae_j=\lambda_j e_j$. Quindi $Imm(A)$ è generata da $\lambda_j e_j$ da cui:

$$\frac{\mathbb{Z}^k}{Imm(A)}=\frac{\bigoplus_j(e_j)}{\bigoplus_j\lambda_j e_j}=\bigoplus_j\frac{e_j}{\lambda_j e_j}=\bigoplus_j\frac{\mathbb{Z}}{\lambda_j\mathbb{Z}}$$

Quindi risulta ovvio che se il determinante è nullo uno dei λ è nullo e dentro la somma diretta si ha una copia di $\mathbb{Z}$ che rende la cardinalità infinita. Invece se tutti sono non nulli il quoziente è il prodotto diretto di tutti i $\mathbb{Z}_{\lambda_j}$ che ha come cardinalità il prodotto dei lambda che corrisponde esattamente al determinante della matrice A.