ESERCIZI DI ALGEBRA 2

FABRIZIO CASELLI

Indice

Parte 1
Esercizi

1. Gruppi ciclici e anelli

Es. 1.1. Stabilire se il gruppo $\mathbb{Z}_{56} \times \mathbb{Z}_{104}$ con l'operazione di somma è ciclico.

Es. 1.2. Sia $\mathcal{U}(\mathbb{Z}_n)$ il gruppo delle classi invertibili modulo n con l'operazione di moltiplicazione. Mostrare che $\mathcal{U}(\mathbb{Z}_8)$ e $\mathcal{U}(\mathbb{Z}_{15})$ non sono ciclici. Mostrare che per ogni $m > 2$ il gruppo $\mathcal{U}(\mathbb{Z}_{m^2-1})$ non é ciclico.

Es. 1.3. Determinare i sottoanelli di $\mathbb{Z}$ e di $\mathbb{Z}_{/n}$, $n > 0$.

Es. 1.4. Determinare i sottoanelli (unitari) di $\mathbb{Z} \times \mathbb{Z}$ e di $\mathbb{Z}_n \times \mathbb{Z}_n$, $n > 0$.

Es. 1.5. Sia Q l'anello dei quaternioni.

(1) dato $\alpha = a + bi + cj + dk$ poniamo $\overline{\alpha} = a - bi - cj - dk$. Mostrare che $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$

(2) dedurre che ogni elemento di Q non nullo é invertibile e che quindi Q é un corpo.

Es. 1.6. Determinare gli elementi invertibili di $\mathbb{Z}[1/n]$.

Es. 1.7. Mostrare che il prodotto diretto di due anelli non banali non è un dominio.

Es. 1.8. In un anello commutativo verificare che gli elementi nilpotenti sono divisori dello 0 e che la somma di nilpotenti è ancora nilpotente.

Es. 1.9. Mostrare che se m ha un divisore quadrato > 1 allora $\mathbb{Z}_{/m}$ non è ridotto (cioè $\mathbb{Z}_{/m}$ ha elementi nilpotenti non nulli).

Es. 1.10. Mostrare che esistono anelli commutativi unitari ridotti (vedi esercizio precedente) che non sono domini.

Es. 1.11. Si consideri la terna $(\mathbb{R} \cup \{+\infty\}, \min, +)$ in cui la "somma" è il "min" e il "prodotto" è il "+". Stabilire quali delle proprietà della definizione di anello commutativo unitario sono soddisfatte e quali no.

Es. 1.12. Sia A un anello non necessariamente commutativo e Z l'insieme degli elementi $a \in A$ tali che $ax = xa$ per ogni $x \in A$. Mostrare che Z è un anello commutativo.

Es. 1.13. Anello di convoluzione. Sia A l'insieme delle funzioni $f : \mathbb{Z}_{>0} \to \mathbb{C}$ con somma data dalla somma ordinaria di funzioni e prodotto $*$ dato da

$$(f * g)(n) = \sum_{h,k>0:\, hk=n} f(h)g(k).$$

Mostrare che tali operazioni danno ad A la struttura di anello.

Es. 1.14. Stabilire se la funzione $f : \mathbb{Z}_{>0} \to \mathbb{C}$ data da $f(n) = 1$ se $n = 1, 2$ e $f(n) = 0$ se $n > 2$ è invertibile nell'anello di convoluzione (vedi esercizio precedente) ed in caso affermativo determinarne l'inversa.

Es. 1.15. Sia A un anello non necessariamente commutativo costituito da elementi idempotenti, cioè taleche $x^2 = x$ per ogni $x \in A$. Mostrare che A è un anello commutativo.

Es. 1.16. Stabilire se l'anello di convoluzione è un dominio.

2. Domini, campi, ideali

Es. 2.1. Mostrare che l'anello delle funzioni continue reali nell'intervallo $[0,1]$ non è un dominio.

Es. 2.2. Mostrare che se V è uno spazio vettoriale di dimensione > 1 allora esistono due endomorfismi non nulli F e G di V tali che $FG = 0$.

Es. 2.3. Sia A un dominio. Mostrare che per ogni $a \neq 0$ la funzione $x \mapsto ax$ è iniettiva da A ad A.

Es. 2.4. Mostrare che in un anello unitario finito un elemento a è invertibile se e solo se $a \neq 0$ e a non è un divisore dello 0 (vedi esercizio precedente). Dedurre che un dominio finito è un campo.

Es. 2.5. Determinare gli elementi invertibili dell'anello di convoluzione (definito nel foglio di esercizi scorso).

Es. 2.6. Mostrare che se A è un anello unitario che contiene un sottoanello unitario K che è anche un campo allora A è (in modo naturale) un K-spazio vettoriale.

Es. 2.7. Dedurre dall'esercizio precedente che se A é un anello unitario finito che contiene un sottoanello K che è anche un campo allora la cardinalità di A è una potenza della cardinalità di K.

Es. 2.8. Un campo K ha solo ideali banali (cioé K e $\{0\}$).

Es. 2.9. Un ideale I di un anello A si dice massimale se $I \neq A$ e l'unico ideale che lo contiene propriamente é A stesso. Mostrare che se A è unitario allora A/I é un campo se e solo se I é massimale.

Es. 2.10. Mostrare che se $f : A \to B$ é un omomorfismo di anelli allora la controimmagine di un ideale di B è un ideale di A. Cosa si può dire dell'immagine di un ideale?

Es. 2.11. Determinare, se possibile, un ideale I di $\mathbb{Z}[X]$ tale che $\mathbb{Z}[X]/I \cong \mathbb{Z}_2$.

Es. 2.12. Sia I l'ideale di $\mathbb{Q}[X]$ dato da tutti i multipli del polinomio $(2X + 3)$. Mostrare esplicitamente che $\mathbb{Q}[X]/I \cong \mathbb{Q}$.

3. Ideali e quozienti

Es. 3.1. Siano I e J ideali di un anello unitario A. Mostrare che se $I + J = A$ allora anche $I^2 + J^2 = A$.

Es. 3.2. Sia $\mathbb{Z}_{(p)}$ l'anello dato dai numeri razionali m/n con $p \not| n$. Mostrare che l'insieme I degli elementi di $\mathbb{Z}_{(p)}$ il cui numeratore è divisibile per p è un ideale. Determinare tutti gli ideali di $\mathbb{Z}_{(p)}$ e dedurre che I è l'unico ideale massimale.

Es. 3.3. Siano A e B anelli unitari e I un ideale di $A \times B$. Mostrare che esistono ideali J di A e M di B tali che $I = J \times M$.

Es. 3.4. Descrivere i possibili quozienti di $\mathbb{Z} \times \mathbb{Z}$ (vedi, se vuoi, l'esercizio precedente).

Es. 3.5. Siano K un campo e

$$A = \left\{ \begin{pmatrix} x & y-x \\ 0 & y \end{pmatrix}, x, y \in K \right\}.$$

– Mostrare che A è un anello (commutativo unitario) con le usuali operazioni di somma e prodotto di matrici.
– Determinare gli elementi invertibili di A;
– Siano I_1 e I_2 gli ideali principali di A generati da $\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$ e da $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ rispettivamente. Mostrare che I_1 e I_2 sono gli unici ideali massimali di A.

Es. 3.6. Sia A l'anello delle funzioni $C^\infty(\mathbb{R})$. Mostrare che le funzioni aventi le prime k derivate nulle in 0 (inclusa la derivata 0-esima) formano un ideale per ogni $k \in \mathbb{N}$.

Es. 3.7. Si consideri l'anello $A = \mathbb{Z}_5[X]/(X^2 - 2X)$.
– Determinare il sottoanello fondamentale di A.
– Mostrare che in ogni classe di A c'è un rappresentante di grado < 2.
– Quanti elementi ha l'anello A?

Es. 3.8. Sia A l'anello dell'esercizio precedente.
– Stabilire se A è un dominio.
– Determinare gli elementi invertibili di A.

Es. 3.9. Sia A l'anello dei due esercizi precedenti.
– Determinare gli ideali di A.
– Determinare i quozienti di A.

Es. 3.10. Dare una descrizione esplicita dell'ideale generato da un sottoinsieme S di un anello non unitario A.

Es. 3.11. Sia A l'anello $\mathbb{C}[X]/(X^2 - X)$.
– Mostrare che

$$\mathcal{U}(A) = \{a(bX - 1) : a, b \in \mathbb{C},\ a \neq 0,\ b \neq 1\}$$

e che se $a(bX - 1) = a'(b'X - 1) \in A$, con $a, a' \neq 0$ e $b, b' \neq 1$ allora $a = a'$ e $b = b'$.

Es. 3.12. Sia A l'anello dell'esercizio precedente. Mostrare che

$$a^n(bX-1)^n = \big(\big((b-1)^n-(-1)^n\big)X+(-1)^n\big)\,a^n.$$

Es. 3.13. Sia A l'anello dei due esercizi precedenti. Mostrare che per ogni $n \geq 1$ esistono esattamente n^2 radici n-esime di 1 in A.

4. Teorema cinese del resto ed estensioni quadratiche

Es. 4.1. Trovare il più piccolo intero positivo k tale che $k \equiv 7 \mod 25$ e $k \equiv 33 \mod 162$;

Es. 4.2. trovare il più piccolo intero positivo k tale che $k \equiv 1 \mod 5$, $k \equiv 2 \mod 7$ e $k \equiv 5 \mod 12$.

Es. 4.3. Determinare tutte le soluzioni dell'equazione $(X-1)(X-7)(2X+1) \equiv 0$ modulo 1635.

Es. 4.4. Determinare tutte le soluzioni intere dell'equazione $2^{X^2-2X} \equiv 1$ modulo 57.

Es. 4.5. (Teorema cinese del resto, un'altra versione) Sia A un anello unitario, I, J ideali tali che $I + J = A$. Dati $a, b \in A$ esiste un elemento $x \in A$ tale che $x \equiv a \mod I$ e $x \equiv b \mod J$.

Es. 4.6. Stabilire per quali valori di $d \in \mathbb{Z}$ si ha che $\mathbb{Z}[\sqrt{d}]$ è un dominio.

Es. 4.7. Stabilire per quali valori di $d \in \mathbb{Z}_{(p)}$ si ha che $\mathbb{Z}_{(p)}[\sqrt{d}]$ è un dominio.

Es. 4.8. Determinare gli elementi invertibili di $\mathbb{Z}_{(p)}[\sqrt{p}]$.

Es. 4.9. Determinare gli elementi invertibili in $\mathbb{Z}[\sqrt{d}]$ per $d < 0$ e per d quadrato.

Es. 4.10. Si consideri il sottoinsieme di $\mathbb{C}$

$$A = \{a + 4bi \mid a, b \in \mathbb{Z}\}$$

(1) Mostrare che A è un sottoanello di $\mathbb{C}$;
(2) Mostrare che -1 non è un quadrato in A;
(3) Mostrare che $A[\sqrt{-1}]$ non è un dominio.

Es. 4.11. Se $d > 0$ non è un quadrato, determinare gli invertibili in $\mathbb{Z}[\sqrt{d}]$ può essere decisamente più complicato. Questo esercizio ha lo scopo di mostrare che

$$\mathcal{U}(\mathbb{Z}[\sqrt{2}]) = \{\pm(1+\varepsilon)^n : n \in \mathbb{Z}\}.$$

Sia $a + \varepsilon b \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$ con $a, b > 0$;
–Mostrare che $b \leq a < 2b$.
– Osservare che l'inverso di $(1+\varepsilon)$ è $(-1+\varepsilon)$.
–Mostrare per induzione su b che $(a+\varepsilon b)(-1+\varepsilon)$ è una potenza di $(1+\varepsilon)$.
–Concludere.

Es. 4.12. Sia $\omega = e^{\frac{4\pi i}{3}} = \cos(\frac{4}{3}\pi) + i\sin(\frac{4}{3}\pi)$ e sia $\mathbb{Z}[\omega]$ l'insieme dei complessi della forma $a + \omega b$, $a, b \in \mathbb{Z}$.
–Mostrare (volendo anche geometricamente) che $\omega^2 + \omega + 1 = 0$.
–Mostrare che $\mathbb{Z}[\omega]$ contiene un sottoanello proprio isomorfo a $\mathbb{Z}[\sqrt{-3}]$.

Es. 4.13. Mostrare che ω^{-1} è contenuto in $\mathbb{Z}[\omega]$.

Es. 4.14. Mostrare che se $\alpha = a + b\omega$ allora $N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2$ e che un elemento è invertibile se e solo se ha norma 1.

Es. 4.15. Le unità di $\mathbb{Z}[\omega]$ sono le radici seste di 1.

Es. 4.16. Mostrare che l'ideale $(2,\varepsilon)$ in $\mathbb{Z}[\sqrt{0}]$ non è principale. Mostrare che l'ideale $(2,\varepsilon)$ in $\mathbb{Z}[\sqrt{-1}]$ è principale.

Es. 4.17. Mostrare che $\mathbb{Z}_5[\sqrt{2}]$ e $\mathbb{Z}_5[\sqrt{3}]$ sono campi isomorfi.

5. Primi, irriducibili, domini euclidei

Es. 5.1. Trovare una radice quadrata di -1 nei seguenti campi: $\mathbb{Z}_5$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{17}$, $\mathbb{Z}_3[\sqrt{2}]$, $\mathbb{Z}_7[\sqrt{3}]$, $\mathbb{Z}_{11}[\sqrt{2}]$.

Es. 5.2.
Sia A un dominio, $a, a', b, b' \in A$ con a, a' associati tra loro e b, b' associati tra loro. È vero che $a + b$ e $a' + b'$ sono associati? È vero che ab e $a'b'$ sono associati?

Es. 5.3. Mostrare che se in un dominio A tutti gli elementi non nulli sono associati tra loro allora A è un campo.

Es. 5.4. Per ciascuna delle seguenti coppie (α, β) di elementi di $\mathbb{Z}[i] := \mathbb{Z}[\sqrt{-1}]$, stabilire se $\alpha|\beta$ o $\beta|\alpha$: $(5, 3 + 4i)$, $(3 + i, 2 + 4i)$, $(5 + i, 5 - i)$, $(17 + i, 13 + 7i)$.

Es. 5.5. Mostrare che se $d > 1$ é un intero dispari allora $\mathbb{Z}[\sqrt{-d}]$ contiene elementi irriducibili che non sono primi.

Es. 5.6. Sia $d > 0$ un intero pari tale che $d + 1$ non é primo. Stabilire se in $\mathbb{Z}[\sqrt{-d}]$ ci sono elementi irriducibili che non sono primi.

Es. 5.7. Sia $I = (3 + i, 1 + 5i) \subset \mathbb{Z}[i]$.
– Trovare tutti gli elementi $\alpha \in \mathbb{Z}[i]$ tali che $I = (\alpha)$;
– Mostrare che per ogni $a \in \mathbb{Z}[i]$ si ha $a \in I$ oppure $a - 1 \in I$;
– Concludere che $\mathbb{Z}[i]/I$ è un campo con due elementi.

Es. 5.8. Se I è un ideale non nullo di $\mathbb{Z}[i]$, l'anello quoziente $\mathbb{Z}[i]/I$ è finito.

Es. 5.9. Dimostrare che $\mathbb{Z}[\sqrt{3}]$ è un anello euclideo (sugg. utilizzare il valore assoluto della norma).

Es. 5.10. Sia $\omega = e^{\frac{2\pi i}{3}}$ e $\mathbb{Z}[\omega]$ l'insieme dei numeri che si scrivono nella forma $a + b\omega$, $a, b \in \mathbb{Z}$. Mostrare che $\mathbb{Z}[\omega]$ è (isomorfo ad un) sottoanello di $\mathbb{Q}[\sqrt{-3}]$ e utilizzando la norma in $\mathbb{Q}[\sqrt{-3}]$ verificare che $\mathbb{Z}[\omega]$ è un anello euclideo.

Es. 5.11. Mostrare che un elemento $a + ib \in \mathbb{Z}[i]$ appartiene all'ideale $(1 + i)$ se e solo se a e b hanno la stessa parità.

Es. 5.12. Sia $I = (8 + i, 4 + 13i) \subset \mathbb{Z}[i]$. Mostrare che $a + ib \in I$ se e solo se $2a \equiv b \mod 5$ e concludere che $\mathbb{Z}[i]/I$ è un campo con 5 elementi.

Es. 5.13. Sia A un dominio euclideo. Mostrare che il quoziente e il resto sono univocamente determinati nelle divisione euclidea se e solo se per ogni $a, b \in A$ si ha $\rho(a - b) \leq \max\{\rho(a), \rho(b)\}$.

6. MCD

Es. 6.1. Determinare un MCD delle seguenti coppie (α, β) di elementi di $\mathbb{Z}[i]$: $(5, 3+4i)$, $(3+i, 2+4i)$,

Es. 6.2. Determinare un MCD delle seguenti coppie (α, β) di elementi di $\mathbb{Z}[i]$: $(5+i, 5-i)$, $(17+i, 13+7i)$.

Es. 6.3. Dimostrare che un primo $p \in \mathbb{Z}$ è irriducibile in $\mathbb{Z}[\sqrt{-2}]$ se e solo se non esistono $a, b \in \mathbb{Z}$ tali che $p = a^2 + 2b^2$.

Es. 6.4. Dimostrare che se $a, b \in \mathbb{Z}$ sono tali che $a^2 + 2b^2$ è primo allora $a + b\sqrt{-2}$ è irriducibile in $\mathbb{Z}[\sqrt{-2}]$. Determinare tutti gli elementi irriducibili di $\mathbb{Z}[\sqrt{-2}]$ di norma al piú 10.

Es. 6.5. Mostrare che -4 è un quadrato in $\mathbb{Z}_p$ se e solo se $p = 2$ oppure $p \equiv 1 \mod 4$.

Es. 6.6. Usando eventualmente anche l'esercizio precedente, determinare quali primi p rimangono primi anche nel dominio $\mathbb{Z}[\sqrt{-4}]$.

Es. 6.7. Dimostrare che 2 è irriducibile in $\mathbb{Z}[\sqrt{-6}]$ ma non è un elemento primo. Fare lo stesso con 5 al posto di 2.

Es. 6.8. Dimostrare che gli elementi 10 e $4 + 2\varepsilon$ non hanno MCD in $\mathbb{Z}[\sqrt{-6}]$.

Es. 6.9. Se A è euclideo e I un ideale non nullo allora I è contenuto in un numero finito di ideali.

Es. 6.10. Sia $I_1 \subseteq I_2 \subseteq \cdots$ una catena infinita di ideali di un anello A. Mostrare che $I = \cup I_i$ è ancora un ideale di A.

Es. 6.11. Un controesempio. Per ogni successione $\alpha = (\alpha_1, \alpha_2, \ldots)$ di numeri naturali consideriamo il "monomio infinito" $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots$ nelle infinite variabili $x_1, x_2, \ldots$ e consideriamo l'insieme A dato dalle combinazioni lineari finite di "monomi infiniti" con coefficienti interi, cioè

$$A = \{n_1 M_1 + \cdots + n_k M_k : k \geq 0, \, n_i \in \mathbb{Z}, \, M_i \text{ monomi infiniti}\}$$

con somma e prodotto definiti in modo naturale. Mostrare che A è un dominio e che esiste una catena infinita di ideali $I_1 \subset I_2 \subset \cdots$ strettamente contenuti uno dentro l'altro.

Es. 6.12. Consideriamo l'anello A dell'esercizio precedente. Mostrare che A contiene elementi non nulli e non invertibili che non possono essere espressi come prodotto di un numero finito di elementi irriducibili.

Es. 6.13. Determinare la fattorizzazione in elementi irriducibili in $\mathbb{Z}[i]$ di $5 + 6i$, di 24 e di $6 + 4i$.

Es. 6.14. Sia $\eta = \frac{1+\sqrt{19}i}{2}$. Osservare che $\eta^2 = \eta - 5$ e dedurre che

$$A = \{a + b\eta : \, a, b \in \mathbb{Z}\}$$

è un sottoanello di $\mathbb{C}$. Nei prossimi punti vogliamo mostrare che A non è un dominio euclideo.

(a) Mostrare che gli unici elementi invertibili dell'anello A sono ± 1.
(b) Mostrare che 2 e 3 sono irriducibili in A.
(c) Supponendo che A sia euclideo con valutazione euclidea ρ mostrare che se α minimizza la ρ tra tutti i ninz di A allora $\alpha = \pm 2, \pm 3$.
(d) Supponendo che A sia euclideo con valutazione euclidea ρ mostrare che se α minimizza la ρ tra tutti i ninz di A allora la divisione euclidea di η per α porta ad una contraddizione.

Es. 6.15. Sia B un dominio e A un sottoanello di B che é anche un PID. Mostrare che per ogni $a_1, a_2 \in A$ esiste $MCD_B(a_1, a_2)$ e $MCD_A(a_1, a_2) = MCD_B(a_1, a_2)$.

7. Riducibili

Es. 7.1. Mostrare che se un primo p è congruo a 5 o 7 modulo 8 allora p è irriducibile in $\mathbb{Z}[\sqrt{-2}]$.

Es. 7.2. Sia p un primo tale che $p-2$ è un quadrato modulo p. Mostrare che p è riducibile in $\mathbb{Z}[\sqrt{-2}]$.

Es. 7.3. Determinare tutte le terne pitagoriche della forma $(a, b, 425)$.

Es. 7.4. Determinare in quanti modi diversi si può scrivere 5625 come somma di due quadrati.

Es. 7.5. Più in generale siano $p \equiv 1 \mod 4$ e $q \equiv 3 \mod 4$ primi. Determinare in quanti modi distinti si può scrivere p^4q^2 come somma di due quadrati.

Es. 7.6. Vogliamo mostrare in questo esercizio che se un anello A è ridotto, cioè non ha elementi nilpotenti, allora in $A[X]$ gli unici elementi invertibili sono le costanti invertibili. Supponiamo quindi che $f = \sum a_i X^i$ e $g = \sum b_j X^j$ siano polinomi in $A[X]$ non (entrambi) costanti tali che $fg = 1$, $n = \deg f$ e $m = \deg g$ e supponiamo senza perdita di generalità che $n \geq m$.

(1) Mostrare che b_0 è invertibile;
(2) Mostrare che $a_n b_m = 0$;
(3) Mostrare che se $m \geq 1$ allora $a_n^2 b_{m-1} = 0$;
(4) Mostrare per induzione su k che $a_n^{k+1} b_{m-k} = 0$ per ogni $k \leq m$;
(5) Concludere che a_n è nilpotente.

Es. 7.7. Siano $m, n > 0$, $m \neq n$. Mostrare che $(m^2 - n^2, 2mn, m^2 + n^2)$ é una terna pitagorica

Es. 7.8. Mostrare che la terna pitagorica dell'esercizio precedente é primitiva se e solo se $MCD(m, n) = 1$ e uno tra m e n é pari

Es. 7.9. Mostrare che se (a, b, c) é una terna pitagorica primitiva (con a dispari) allora esistono m ed n tali che $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$. (osservare $(c+a)(c-a) = b^2$), mostrare che $c + a$ e $c - a$ hanno in comune solo un fattore 2...)

Es. 7.10. Sia b pari. Mostrare che esiste una terna pitagorica primitiva (a, b, c) se e solo se $b \equiv 0 \mod 4$

Es. 7.11. Sia a dispari. Mostrare che esiste una terna pitagorica primitiva (a, b, c). (Osservare che $a = (\frac{a+1}{2} + \frac{a-1}{2})(\frac{a+1}{2} - \frac{a-1}{2})$)

8. Polinomi

Es. 8.1. Siano $f = X^3 + X - 1$ e $g = X^2 + 1$ polinomi in $\mathbb{Q}[X]$. Determinare $q, r \in \mathbb{Q}[X]$ con $\deg r < \deg g$ tali che $f = qg + r$.

Es. 8.2. Se K è un campo un polinomio in $K[X]$ di grado 5 senza radici che non è irriducibile è il prodotto di un irriducibile di grado 2 e uno irriducibile di grado 3.

Es. 8.3. Se K è un campo mostrare che esistono infiniti polinomi irriducibili monici in $K[X]$.

Es. 8.4. Trovare il MCD tra le seguenti coppie di polinomi
– $X^2 + 1$ e $X^5 + 1$ in $\mathbb{Z}_2[X]$;
– $X^2 - X + 4$ e $X^3 + 2X^2 + 3X + 2$ in $\mathbb{Z}_3[X]$;
– $X^6 - 1$ e $X^7 - 2X^3 + 3X^2 - 2X + 1$ in $\mathbb{Q}[X]$
– $X^9 - 1$ e $X^{11} - 1$ in $\mathbb{Q}[X]$;
– $X^8 + 6X^6 - 8X^4 + 1$ e $X^{12} + 7X^{10} - 3X^8 - 3X^2 - 2$ in $\mathbb{Q}[X]$.

Es. 8.5. Per le seguenti coppie (f, g) di polinomi in $\mathbb{Q}[X]$ trovare due polinomi $s, t \in \mathbb{Q}[X]$ tali che $sf + tg$ sia un MCD tra f e g
– $(X^2 - 3X + 2, X^2 + X + 1)$
– $(2X^3 - 7X^2 + 7X - 2,\ 2X^3 + X^2 + X - 1)$

Es. 8.6. Il polinomio $X^4 + X^3 + X + 1$ è riducibile in ogni campo K.

Es. 8.7. Stabilire se $X^4 + 1$ è irriducibile in $\mathbb{Q}[X]$.

Es. 8.8. Dimostrare che se $f \in K[X]$ e $a \in K$ allora $f \equiv \tilde{f}(a) \mod (X - a)$. Stabilire se questo risultato è vero in un anello (commutativo unitario) qualsiasi.

9. Campo delle frazioni e polinomi irriducibili

Es. 9.1. Determinare un generatore dei gruppi $(\mathbb{Z}_{/5}[\sqrt{2}])^*$ e $(\mathbb{Z}_{/29})^*$.

Es. 9.2. Sia A un dominio e K un campo, $A \subset K$. Supponiamo che per ogni $k \in K$ esiste $a \in A$ tale che $ka \in A$. Mostrare che K è isomorfo a $Q(A)$, il campo delle frazioni di A.

Es. 9.3. Determinare il campo delle frazioni di $\mathbb{Z}[\sqrt{d}]$ per ogni d non quadrato;

Es. 9.4. Descrivere il campo delle frazioni di $\mathbb{Z}[X]$ e di $\mathbb{Z}_p[X]$.

Es. 9.5. Detto $L = \mathbb{Z}_p(X)$ il campo dei quozienti di $\mathbb{Z}_p[X]$ e $K = \mathbb{Z}_p(X^p)$ si consideri il polinomio $f = Y^p - X^p \in K[Y]$. Mostrare che f è irriducibile in $K[Y]$, ma che ha radici multiple in L.

Es. 9.6. Stabilire se il polinomio $X^3 + (-3+2i)X^2 + (3+4i)X - 17 - 6i$ è irriducibile in $(\mathbb{Q}[i])[X]$.

Es. 9.7. Sia K un campo, $K \subset \mathbb{C}$; due polinomi in $K[X]$ sono relativamente primi in $K[X]$ sse non hanno radici in comune in $\mathbb{C}$.

Es. 9.8. Sia K un campo. Allora
– $X^3 + 2$ e $X + 1$ sono coprimi in $K[X]$;
– $X^3 - 2$ e $X + 1$ sono coprimi in $K[X]$ se e solo se $car(K) \neq 3$;
– $X^3 - 2$ e $X^2 + X$ sono relativamente primi in $K[X]$ se e solo se $car(K) \neq 2, 3$.

Es. 9.9. Stabilire se i seguenti polinomi hanno radici multiple in $\mathbb{C}$: $X^4 + X$, $X^5 - 5X + 1$, $X^5 + X^4 + 2X^3 + 2X^2 + X + 1$.

Es. 9.10. Sapendo che il polinomio $f(X) = X^4 - 4X^3 + 3X^2 + 14X + 26$ ha come radici complesse $3 + 2i$ e $-1 - i$ decomporre f in $\mathbb{R}[X]$ e in $\mathbb{C}[X]$.

Es. 9.11. Determinare le radici razionali dei polinomi $X^4 - X^3 + X - 1$ e $2X^4 - 4X + 3$.

Es. 9.12. Dimostrare che i seguenti polinomi sono irriducibili in $\mathbb{Q}[X]$.
– $2X^4 - 8X^2 + 1$;
– $X^4 + X + 1$;
– $X^4 + 3x + 5$;
– $3X^4 + 2X^3 + 4X^2 + 5X + 1$; – $X^5 + 5X^2 + 4X + 7$;
– $15X^5 - 2X^4 + 15X^2 - 2X + 15$

Es. 9.13. Stabilire se i seguenti polinomi sono irriducibili in $\mathbb{Q}[X]$:
– $X^3 - X + 1$;
– $X^3 + 2X + 10$;
– $X^3 - X - 1$;
– $X^3 - 2X^2 + X + 15$;
– $X^4 + 2$;
– $X^4 - 2$;
– $X^4 + 4$;
– $X^4 - X + 1$;

Es. 9.14. Scomporre in fattori irriducibili $X^n - 1$ con $n = 6, 8, 12, 24$ in $\mathbb{Q}[X]$.

Es. 9.15. Mostrare che due polinomi interi sono relativamente primi in $\mathbb{Q}[X]$ sse l'ideale che essi generano in $\mathbb{Z}[X]$ contiene un intero non nullo.

10. Radici

Es. 10.1. Mostrare che $\sqrt{2}$, $\sqrt{2}+1$, $\sqrt{2}+\sqrt{3}$, $\sqrt{2}+\sqrt[3]{3}$ e $\sqrt{2}+\sqrt{3}+\sqrt{5}$ sono algebrici (cioé sono radici di un polinomio non nullo in $\mathbb{Z}[X]$.

Es. 10.2. Sia $\alpha \in \mathbb{C}$ una radice del polinomio $f = X^4 - 3X - 5$.
–Provare che f è irriducibile in $\mathbb{Q}[X]$.
–Trovare il polinomio minimo di $2\alpha - 3$ su $\mathbb{Q}$.
–Trovare il polinomio minimo di α^2 su $\mathbb{Q}$.

Es. 10.3. Mostrare che se A è un dominio allora per ogni $a \in A$, $a \neq 0$ e per ogni $d, n \in \mathbb{N}$ tali che $d|n$ si ha

$$a^d - 1 | a^n - 1.$$

Dedurre che se K è un campo e $d|n$ allora per ogni $m \in \mathbb{N}$

$$X^{(m^d)} - X | X^{(m^n)} - X.$$

Es. 10.4. Sia $A = \mathbb{Z}$ oppure $A = K[X]$, $a \in A$ ninz. Siano $d, n > 0$ tali che $a^d - 1 | a^n - 1$. Mostrare che $d|n$.

Es. 10.5. – Mostrare che per ogni $n \geq 1$ esiste un polinomio $f \in \mathbb{Q}[X, Y]$ tale che $\sin(n\alpha) = f(\sin(\alpha), \cos(\alpha))$ per ogni $\alpha \in \mathbb{R}$.
– Mostrare che per ogni $n \geq 1$ e per ogni $\alpha \in \mathbb{R}$ esistono due polinomi $g, h \in \mathbb{Q}[X]$ tali che $\sin(n\alpha) = g(\sin(\alpha)) + \sqrt{1 - \sin^2(\alpha)}h(\sin(\alpha))$.
– Dedurre che $\sin(1°)$ è algebrico su $\mathbb{Q}$.

Es. 10.6. Sia $f = 2X^4 - 41X^3 + 201X^2 - 71X - 91$.
– Sapendo che f ammette tre radici distinte intere positive, determinare la fattorizzazione in irriducibili di f in $\mathbb{Z}[X]$;
– Determinare il numero di radici di f in $\mathbb{Z}_{/1635}$, ed esibire almeno 5 soluzioni distinte.

11. Costruzioni con riga e compasso

Es. 11.1. Sia $\theta = \frac{2\pi}{5}$.

(1) Sfruttando le formule per il seno e coseno di somme di archi cioé
- $\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$
- $\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$,

con $\alpha = \theta$ e $\beta = 4\theta$ mostrare che $\cos\theta$ é una radice del polinomio $f = 16X^4 - 12X^2 + 1$.

(2) Mostrare che il polinomio f é riducibile e dedurre che é possibile costruire con riga e compasso un pentagono regolare.

Es. 11.2. Sia $n > 0$. Mostrare che é possibile costruire un poligono regolare con n lati se e solo se é possibile costruire un poligono regolare con $2n$ lati.

Es. 11.3. Sia $\theta = \frac{2\pi}{28}$.

(1) Mostrare che é possibile costruire un poligono regolare con 28 lati se e solo se $\cos\theta$ é costruibile.
(2) Mostrare che $\mathbb{Q}[e^{i\theta}] = \mathbb{Q}[\cos\theta, \sin\theta, i]$.
(3) Mostrare che $\left[\mathbb{Q}[e^{i\theta}] : \mathbb{Q}[\cos\theta]\right]$ é una potenza (piccola) di 2.
(4) Determinare il grado del polinomio minimo di $e^{i\theta}$ su $\mathbb{Q}$ e dedurre che non é possibile costruire con riga e compasso un ettagono regolare.

Es. 11.4. (1) Scrivere $\sin(3\theta)$ in funzione di $\cos\theta$.
(2) Applicando il punto precedente a $\theta = 20°$ mostrare che $\cos 20°$ é radice di un polinomio irriducibile in $\mathbb{Q}[X]$ di grado 3.
(3) Concludere che é impossibile trisecare l'angolo di $60°$ con riga e compasso.

12. Campo di spezzamento

Es. 12.1. Determinare un campo di spezzamento K di $X^3+\sqrt{2}X+1$ su $\mathbb{Q}[\sqrt{2}]$ e il grado $[K:\mathbb{Q}[\sqrt{2}]]$.

Es. 12.2. Sia $f=(X^{15}-1)(X^{12}-1)$. Determinare il campo di spezzamento di f su $\mathbb{Z}_2$ e su $\mathbb{Z}_7$.

Es. 12.3. Sia $a\in\mathbb{Z}_7^*$ e $f=(X^4-a)(X^4+a)\in\mathbb{Z}_7[X]$. Dimostrare che un campo di spezzamento di f su $\mathbb{Z}_7$ ha 49 elementi.

Es. 12.4. Determinare il grado del campo di spezzamento su $\mathbb{Q}$ dei seguenti polinomi

- X^2+X+1;
- X^5-1;
- X^5-2

Es. 12.5. Determinare il grado del campo di spezzamento su $\mathbb{Z}_{/5}$ dei seguenti polinomi

- X^2+X+1;
- X^5-1;
- X^5-2

Es. 12.6. Sia $f=X^3-3X-1\in\mathbb{Q}[X]$.
– Verificare che f è irriducibile.
– Detta α una sua radice complessa scrivere $(2\alpha^2-\alpha-4)^2$ come combinazione lineare di $1,\alpha,\alpha^2$.
–Verificare che $\mathbb{Q}[\alpha]$ è il campo di spezzamento di f su $\mathbb{Q}$.

Es. 12.7. Sia p un primo e consideriamo il polinomio $f=X^n-1$ su $\mathbb{Z}_p$. Sia inoltre $\mathbb{F}_{p^k}$ il suo campo di spezzamento.
– Verificare che le radici di f formano un sottogruppo moltiplicativo (ciclico) di $\mathbb{F}_{p^k}^*$
– Osservare che se $n=p^h r$ con $p\not| r$ allora $\mathbb{F}_{p^k}$ è anche il campo di spezzamento di X^r-1.
– Concludere che k è la più piccola soluzione positiva dell'equazione $p^k\equiv 1 \mod r$.

Es. 12.8. Sia $f=x^9-1$.
– Calcolare il campo di spezzamento di f su $\mathbb{Z}_{11}$.
– Mostrare che f ha un fattore irriducibile di grado 6 su $\mathbb{Z}_{11}$.

Es. 12.9. Determinare il campo di spezzamento di $f=X^4+X^2+1$ su $\mathbb{Q}$.

Es. 12.10. Sia p un primo. Determinare il grado del campo di spezzamento di X^p-1 su $\mathbb{Q}$.

Es. 12.11. Per ogni $n\in\mathbb{N}$ e per ogni primo p descrivere e determinare il grado del campo di spezzamento di X^n-p su $\mathbb{Q}$.

13. Galois

Es. 13.1. Sia $K \subseteq \mathbb{C}$ e $f \in K[X]$. Sia L un campo di spezzamento di f su K. Mostrare che il gruppo di Galois $Gal(L/K)$ é isomorfo ad un sottogruppo del gruppo simmetrico S_n.

Es. 13.2. Determinare $Gal(\mathbb{C}/\mathbb{R})$.

Es. 13.3. Siano $m, n > 0$. Mostrare che $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$ se e solo se mn é un quadrato.

Es. 13.4. Sia $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Mostrare che $L/\mathbb{Q}$ é normale e che $Gal(L/K) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Determinare tutti i campi intermedi F tali che $\mathbb{Q} \subseteq F \subseteq L$.

Es. 13.5. Sia $\zeta = e^{\frac{2\pi i}{5}}$ una radice primitiva quinta di 1 e $L = \mathbb{Q}[\zeta]$;

- mostrare che $L/\mathbb{Q}$ é un'estensione normale di grado 4;
- mostrare che $Gal(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ dove σ_i é univocamente determinata da
$$\sigma_i(\zeta) = \zeta^i;$$
- mostrare che σ_2 ha ordine maggiore di 2 e dedurre che $Gal(L/\mathbb{Q}) \cong \mathbb{Z}_{/4}$;
- mostrare che esiste un unico campo intermedio F tale che $\mathbb{Q} \subsetneq F \subsetneq L$;
- mostrare che σ_4 coincide con il coniugio complesso (ristretto ad L) per cui ha ordine 2. Detto $H = \{\sigma_1, \sigma_4\}$ dedurre che il campo intermedio é $F = L \cap \mathbb{R}$;
- ricordando (o dopo aver osservato) che $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ mostrare che $\zeta + \zeta^4$ é una radice del polinomio $X^2 + X - 1$ e dedurre che $F = \mathbb{Q}[\sqrt{5}]$.

Es. 13.6. Usare l'esercizio precedente per osservare che $i \notin \mathbb{Q}[e^{\frac{2\pi i}{5}}]$ e dedurre che $1 + X + X^2 + X^3 + X^4$ é irriducibile su $\mathbb{Q}[i]$.

Es. 13.7. Generalizziamo un precedente esercizio. Sia $n > 0$ e $\zeta = e^{\frac{2\pi i}{n}}$ e $L = \mathbb{Q}[\zeta]$.

(1) Mostrare che $L/\mathbb{Q}$ é un'estensione normale;
(2) per ogni $i < n$ con $MCD(i, n) = 1$ poniamo σ_i l'unico $\mathbb{Q}$-isomorfismo di L tale che $\sigma_i(\zeta) = \zeta^i$; mostrare che $Gal(L/\mathbb{Q}) = \{\sigma_i : i < n, MCD(i, n) = 1\}$;
(3) mostrare che $Gal(L/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}_{/n})$.

Es. 13.8. determinare $Gal(L/\mathbb{Q})$ dove L é il campo di spezzamento di $X^3 - 2$.

Es. 13.9. sia $f = X^5 - 4X + 2$, L il suo campo di spezzamento su $\mathbb{Q}$ e $G = Gal(L/\mathbb{Q})$.

(1) ricordando che $G \leq S_5$ mostrare che G contiene un 5-ciclo (ricorda che i 5-cicli sono gli unici elementi di ordine 5 in S_5);
(2) calcolare $f'(X)$, $f(0)$ e $f(1)$ e dedurre che f ha esattamente due radici non reali (coniugate tra loro);
(3) dedurre dal punto precedente che G contiene una trasposizione;
(4) concludere che $G = S_5$.

Es. 13.10. Siano $\mathbb{Q} \subseteq K \subseteq L$ con K, L estensioni normali di $\mathbb{Q}$, $[L : K] = 2$, $L = K[\alpha]$ con $\alpha^2 \in \mathbb{Q}$. Allora
$$Gal(L/\mathbb{Q}) \cong Gal(K/\mathbb{Q}) \times \mathbb{Z}_{/2}.$$

Es. 13.11. per ogni $m > 0$ sia L il campo di spezzamento di $(X^4+1)(X^2-m)$. Determinare $Gal(L/\mathbb{Q})$;

Es. 13.12. Sia $f \in \mathbb{Q}[X]$ un polinomio irriducibile, α_1, α_2 due radici complesse distinte di f. Mostrare che $\alpha_1 - \alpha_2 \notin \mathbb{Q}$. (suggerimento: considerare σ nel gruppo di Galois tale che $\sigma(\alpha_1) = \alpha_2$)

Es. 13.13. (una vecchia promessa) Sia $\rho : \mathbb{Z}[X] \to \mathbb{Z}_{/2}[X]$ la riduzione modulo 2 dei coefficienti. Sia $f \in \mathbb{Z}[X]$ di grado n monico tale che $\rho(f)$ sia irriducibile. Sia $\alpha \in \mathbb{C}$ una radice di f.

(1) Determinare un polinomio $g \in \mathbb{Z}[X]$ monico di grado n tale che $g(\alpha^2) = 0$;
(2) mostrare che $\rho(g) = \rho(f)$ (potrá essere utile considerare una radice di $\rho(f)$ nel suo campo di spezzamento su $\mathbb{Z}_{/2}$;
(3) concludere che g é irriducibile ed é quindi il polinomio minimo di α^2).

Es. 13.14. Identifichiamo il piano delle costruzioni con riga e compasso con il piano complesso. Diciamo che un numero complesso $z = a + ib$ é costruibile se il punto corrispondente é costruibile (e sappiamo che questo é equivalente a richiedere che a e b sono entrambi costruibili)

(1) sia $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$. Mostrare che z é costruibile se e solo se lo sono sia r che $\cos\theta$ che $\sin\theta$;
(2) mostrare che i numeri complessi costruibili formano un campo;
(3) mostrare che se z é costruibile e $w^2 = z$ allora anche w é costruibile;
(4) concludere che z é costruibile se e solo se esiste una catena di campi
$$Q = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$
tali che $[K_i : K_{i-1}] = 2$ per ogni i e $z \in K_n$.

Es. 13.15. Sia $n = 4.294.967.295$. Fattorizzare n in numeri primi.

E' uno scherzo, vi do io questa fattorizzazione: é $n = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$. Vogliamo mostrare che é possibile costruire un poligono regolare con n lati con riga e compasso.

(1) osservare che per un esercizio precedente $L = \mathbb{Q}[e^{\frac{2\pi i}{n}}]$ é un'estensione normale di $\mathbb{Q}$;
(2) mostrare che per un esercizio precedente si ha che $|Gal(L/\mathbb{Q})|$ é una potenza di 2 (usando che $2^{16} = 65.536$);
(3) ricordando che se un gruppo G ha ordine p^n con p primo allora esistono sottogruppi $H_0 \leq H_1 \leq \cdots \leq H_n = G$ con $|H_i| = p^i$ per ogni i mostrare che $e^{\frac{2\pi i}{n}}$ é costruibile.
(4) Commento: n é il piú grande numero dispari noto per cui é possibile costruire un poligono regolare con n lati!

Es. 13.16. Un primo di Fermat é un numero primo della forma $2^k + 1$. Mostrare che é possibile costruire un poligono regolare con n lati se e solo se n é della forma $n = 2^r p_1 \cdots p_k$ dove i p_i sono primi di Fermat dispari distinti. Il commento dell'esercizio precedente segue dal fatto che gli unici primi di Fermat noti sono 2,3,5,17,257, 65537.

Es. 13.17. Mostrare che se $2^k + 1$ é primo allora k é una potenza di 2 (suggerimento: per d dispari utilizzare l'identitá $a^d + 1 = (a+1)(a^{d-1} - a^{d-2} + a^{d-3} - \cdots + 1)$).

Parte 2
Soluzioni

. Soluzioni: Gruppi ciclici e anelli

Es. 1.1 Non é ciclico per il teorema cinese del resto. Possiamo anche osservare che possiede due elementi e quindi due sottogruppi di ordine 2 (quali?).

Es. 1.2 Anche qui basta trovare due elementi distinti di ordine 2: questi sono m e $-m$.

Es. 1.3 Siccome un sottoanello deve contenere 1 allora sia $\mathbb{Z}$ che $\mathbb{Z}_{/n}$ non hanno sottoanelli propri. Se consideriamo sottoanelli non unitari allora osserviamo che i sottogruppi additivi sono chiusi rispetto al prodotto e quindi sono anche sottoanelli: per $\mathbb{Z}$ abbiamo $n\mathbb{Z}$ per ogni $n \geq 0$ e per $\mathbb{Z}_{/m}$ abbiamo $d\mathbb{Z}_{/m}$ per ogni $d|m$.

Es. 1.4 I sottoanelli di $\mathbb{Z} \times \mathbb{Z}$ sono i seguenti: per ogni $m \geq 0$ poniamo

$$H_m = \{(a,b) : a \equiv b \mod m\}.$$

Infatti questi H_m sono effettivamente sottoanelli unitari (contengono 1=(1,1) e sono chiusi per differenza e prodotto). Mostriamo che sono tutti fatti in questo modo: sia quindi H un sottoanello di $\mathbb{Z} \times \mathbb{Z}$ e sia m il minimo intero positivo tale esiste $(a,b) \in H$ con $a - b = m$. (Se tale m non esiste allora $H = H_0$). Si mostra a questo punto la doppia inclusione tra H e H_m. In $\mathbb{Z}_{/n} \times \mathbb{Z}_{/n}$ si ha analogamente che i sottoanelli sono dati da $K_d = \{([a],[b]) : a \equiv b \mod d\}$ al variare di d tra i divisori di n.

Es. 1.5 Nelle dispense

Es. 1.6 Sia $n = p_1^{m_1} \cdots p_r^{m_r}$ dove i p_i sono primi. Mostriamo che

$$\mathcal{U}(\mathbb{Z}[1/n]) = \{p_1^{a_1} \cdots p_r^{a_r} : a_1, \ldots, a_r \in \mathbb{Z}\}.$$

Vediamo la doppia inclusione:
$\subseteq$: sia $\frac{a}{n^k} \in U(\mathbb{Z}[1/n])$ con a intero e $k \geq 0$.Allora per definizione esistono b intero e $h \geq 0$ tali che

$$\frac{a}{n^k} = \frac{n^h}{b}$$

e quindi $ab = n^{h+k}$; da questo fatto segue che i primi che dividono a sono anche divisori di n e quindi $a = p_1^{b_1} \cdots p_r^{b_r}$ e concludiamo che

$$\frac{a}{n^k} = p_1^{b_1 - km_1} \cdots p_r^{b_r - km_r}$$

$\supseteq$: sia $x = p_1^{a_1} \cdots p_r^{a_r}$ mostriamo che x appartiene a $\mathbb{Z}[1/n]$ e che è invertibile. Sia $k > 0$ abbastanza grande tale che $km_i + a_i > 0$ per ogni i. Allora

$$x = p_1^{a_1} \cdots p_r^{a_r} = \frac{p_1^{a_1+km_1} \cdots p_r^{a_r+km_r}}{p_1^{km_1} \cdots p_r^{km_r}} = \frac{a}{n^k}$$

dove $a \in \mathbb{Z}$ per la scelta di k. In particolare $x \in \mathbb{Z}[1/n]$ e per la stessa ragione $x^{-1} = p_1^{-a_1} \cdots p_r^{-a_r} \in \mathbb{Z}[1/n]$ e quindi $x \in \mathcal{U}(\mathbb{Z}[1/n])$.

Es. 1.7 Basta osservare che se A e B sono anelli non banali dati $a \in A$ e $b \in B$ non nulli si ha $(a,0) \cdot (0,b) = (0,0)$.

Es. 1.8 Se $a^n = 0$ e $b^m = 0$ allora $(a+b)^{n+m-1} = 0$.

Es. 1.9 Sia $d > 1$ tale che $d^2|m$. Allora $\frac{m}{d}$ é nilpotente. Infatti $(m/d)^2 = m \cdot \frac{m}{d^2} = 0 \in \mathbb{Z}_m$. Chiaramente $m/d \neq 0 \in \mathbb{Z}_m$ perché $0 < m/d < m$.

Es. 1.10 Se m non ha fattori quadrati maggiori di 1 allora $\mathbb{Z}_m$ è ridotto. Sia infatti $m = p_1 \cdots p_r$ dove i p_i sono primi distinti. Se a è nilpotente in $\mathbb{Z}_m$ allora $a^n = 0 \in \mathbb{Z}_m$ e quindi $m|a^n$. In particolare $p_i|a^n$ per ogni i e quindi $p^i|a$ per ogni i. Concludiamo che $m|a$ cioè $a = 0 \in \mathbb{Z}_m$.

Es. 1.11 da scrivere

Es. 1.12 Siano $a, b \in Z$ e $x \in A$. Allora $(a-b)x = ax + (-b)x = xa - bx = xa - xb = xa + x(-b) = x(a-b)$ e quindi $a - b \in Z$. Similmente si verifica che $ab \in Z$ e quindi Z è un sottoanello. Che sia commutativo è ovvio.

Es. 1.13 A è un anello unitario. Le uniche proprietà non banali a verificare sono l'esistenza dell'elemento neutro rispetto al prodotto e la proprietà associativa rispetto al prodotto. L' elemento neutro è la funzione e che calcolata in 1 dà 1 e calcolata in $n > 1$ dà 0. La proprietà associativa si verifica osservando che

$$((f * g) * l)(n) = \sum_{h,k,m>0:\, hkm=m} f(h)g(k)l(m) = (f * (g * l)(n)$$

Es. 1.14 f è invertibile e la sua inversa é data da $g(2^m) = (-1)^m$ e $g(n) = 0$ se n non è una potenza di 2. Infatti si verifica facilmente che $(f * g)(n) = 0$ se n non è una potenza di 2 (ogni addendo della convoluzione svanisce),

$$(f * g)(2^m) = f(1)g(2^m) + f(2)g(2^{m-1}) = (-1)^m + (-1)^{m-1} = 0$$

per $m \geq 1$ e $(f * g)(1) = 1$.

Es. 1.15 Osserviamo intanto che $x = -x$ per ogni $x \in A$ infatti $x = x^2 = (-x)^2 = -x$. L'uguaglianza $x^2 = (-x)^2$ non è del tutto ovvia ma segue dal seguente conto dalla proprietà di base che abbiamo visto che $-ab = (-a)b = a(-b)$ da cui $(-x)^2 = (-x)(-x) = -x(-x) = -(-x^2) = x^2$.

Siano ora $x, y \in A$. Abbiamo $x+y = (x+y)^2 = x^2+y^2+xy+yx = x+y+xy+yx$. Uguagliando il primo e l'ultimo membro abbiamo $xy+yx = 0$ da cui $xy = -yx = yx$ sfruttando la prima osservazione che ogni elemento è uguale al proprio opposto.

Es. 1.16 Siano f, g due elementi non nulli dell'anello di convoluzione. Siano n, m minimi tali che $f(n) \neq 0$ e $g(m) \neq 0$ rispettivamente. Allora $f * g(nm) = f(n)g(m) \neq 0$ e quindi $f * g \neq 0$.

. Soluzioni: Domini, campi, ideali

Es. 2.1 Basta scegliere f nulla in $[0, 1/2]$ e g nulla in $[1/2, 0]$.

Es. 2.2 Basta scegliere in dimensione 2 $F = G = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Es. 2.3 Se $ax = ay$ abbiamo $a(x - y) = 0$ da cui $x = y$ perché A perché vale la legge di cancellazione per a.

Es. 2.4 Se a non è divisore dello 0 come nell'esercizio precedente la funzione $x \mapsto ax$ è iniettiva e quindi anche suriettiva perché A è finito. Esiste quindi $x \in A$ tale che $ax = 1$.

Es. 2.5 Sono tutte le f tali che $f(1) \neq 0$.

Es. 2.6 La moltiplicazione di un elemento di A per un elemento di K dà ad A la struttura di K-spazio vettoriale. Osserviamo che se A non è un unitario e contiene un sottoanello isomorfo ad un campo questo non implica che A sia un K-spazio vettoriale. Infatti in tal caso non è vero in generale che, detto 1 l'elemento neutro di K rispetto al prodotto si abbia $1 \cdot a = a$ per ogni $a \in A$. Ad esempio $A = \mathbb{Z}_6$ contiene il sottoanello $\{0, 3\}$ che è isomorfo al campo $\mathbb{Z}_2$. Tuttavia, A non è un uno $\mathbb{Z}_2$-spazio vettoriale.

Es. 2.7 Dall'esercizio A è uno spazio vettoriale su K necessariamente di dimensione finita. Se tale dimensione è n si ha $|A| = |K|^n$ (considerare una base)

Es. 2.8 Un ideale che contiene un elemento invertibile coincide con l'anello stesso. È vero anche il viceversa: se A è un anello unitario non banale che non contiene ideali non banali allora è un campo. Infatti in tal caso se $a \in A$, $a \neq 0$ allora l'ideale (a) generato da a, contenendo a, coincide necessariamente con A. Di conseguenza $a \in (a)$ e quindi a è invertibile.

Es. 2.9 Supponiamo che A/I sia un campo J un ideale che contiene propriamente I. Sia quindi $a \in J$, $a \notin I$. Allora la classe di a è invertibile in A/I e quindi esiste $b \in A$ tale che $1 - ab \in I$. Ma allora $1 = (1 - ab) + ab \in J$ e quindi $J = A$ per cui I è massimale.

Viceversa, sia I massimale. Sia $a \notin I$. Dobiamo mostrare che la classe di a è inveritbile in A/I. Allora l'ideale $(I, a) = \{ab + x : b \in A, x \in I\}$ contenendo propriamente I coincide con A. Esistono quindi $b \in A$ e $x \in I$ tali che $ab + x = 1$. Ma allora la classe di a è invertibile in A/I (e la sua inversa è proprio la classe di b).

Es. 2.10 Sia J un ideale di B e $I = f^{-1}(J)$ la sua controimmagine. Abbiamo $f^{-1}(0) \ni 0 \in I$. Se $x, y \in I$ allora $f(x), f(y) \in J$ e quindi $f(x-y) = f(x) - f(y) \in J$ e quindi $x - y \in I$, e per ogni $a \in A$ abbiamo $f(ax) = f(a)f(x) \in J$ per la proprietà di assorbimento di J e quindi $ax \in I$. L'immagine di un ideale non é in generale un ideale. Ad esempio se $\iota : \mathbb{Z} \to \mathbb{Q}$ è l'inclusione l'immagine dell'ideale $2\mathbb{Z}$ non è un ideale in $\mathbb{Q}$ (che essendo un campo ha solo ideali banali). Si può comunque facilmente verificare che l'immagine di un ideale è sempre un ideale se l'omomorfismo è suriettivo.

Es. 2.11 Vogliamo che $\mathbb{Z}[X]/I$ sia composto da due sole classi. Questo si può realizzare scegliendo I come l'ideale dato da tutti polinomi con termine noto pari (verificare che si tratta effettivamente di un ideale). In questo modo abbiamo la classe nulla data dai polinomi con termine noto pari e l'altra classe data dai polinomi con termine noto dispari.

Es. 2.12 Consideriamo l'omomorfismo

$$\varphi : \mathbb{Q}[X] \to \mathbb{Q}$$

dato da $\varphi(P) = P(-3/2)$. Si verifica immediatamente che φ é un omomorfismo suriettivo e che il nucleo è dato proprio da I. Il teorema fondamentale di omomorfismo ci permette di concludere.

. Soluzioni: Ideali e quozienti

Es. 3.1 Siano $x \in I$ e $y \in J$ tali che $x+y=1$. Allora $1=(x+y)^3=(x^3+3x^2y)+(3xy^2+y^3) \in I^2+J^2$.

Es. 3.2 Dato $k \geq 0$ sia

$$I_k := \{a/b \in A : p^k|a\}.$$

Verificare che gli I_k sono ideali. Sia ora I un qualunque ideale e k minimo tale che esiste $a/b \in I$ con $p^k|a$. Mostrare che $I = I_k$.

Es. 3.3 Mostrare in generale che se I è un ideale di $A \times B$ e $(a,b) \in I$ allora $(a,0)$ e $(0,b) \in I$ dedurre che I è dato dal prodotto di ideali di A e B.

Es. 3.4 Per l'esercizio precedente un ideale di $\mathbb{Z} \times \mathbb{Z}$ è della forma $n\mathbb{Z} \times m\mathbb{Z}$ e il relativo quoziente è $\mathbb{Z}_n \times \mathbb{Z}_m$.

Es. 3.5 Le verifiche che A è un anello sono elementari. Un elemento è invertibile se e solo se x e y sono entrambi non nulli (verificare che in tal caso effettivamente l'inversa sta in A). Se I è un ideale proprio di A non può contenere elementi invertibili e quindi necessariamente si ha $x=0$ oppure $y=0$. Nel primo caso otteniamo $I_1 \subset I$, nel secondo $I_2 \subset I$. Tuttavia se $I_1 \neq I$ abbiamo che I contiene necessariamente un elemento di I_2 e quindi un elemento invertibile. Abbiamo quindi mostrato che I_1 e I_2 sono gli unici ideali propri.

Es. 3.6 Basta ricordare la formula per la derivata k-esima di un prodotto

$$(fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)} g^{(k-i)}.$$

Es. 3.7 Gli elementi di A sono rappresentati da polinomi di grado al più 1, perché $X^2 = 2X \in A$ e quindi ogni volta che abbiamo un monomio della forma X^n con $n \geq 2$ abbiamo $X^n = 2X^{n-1}$. Due polinomi di grado al piú 1 rappresentano due classi distinte perché la differenza tra polinomi distinti di grado al piú 1 non può essere un multiplo di $X^2 - 2X$. Di conseguenza A ha 25 elementi.

Es. 3.8 A non è un dominio (perché $X \cdot (X-2) = 0 \in A$. Gli elementi invertibili di A sono quelli diversi da kX e da $k(X-2$ al variare di $k \in \mathbb{Z}_5$.

Es. 3.9 Gli ideali propri devono contenere solo elementi non invertibili e quindi gli elementi del tipo kX o del tipo $k(X-2)$ con $k \in \mathbb{Z}_5$, ma non elementi di entrambi i tipi altrimenti avremmo anche elementi invertibili. Dedurre che abbiamo esattamente 2 ideali non banali: $I = \{kX : k \in \mathbb{Z}_5\}$ e $J = \{k(X-2) : k \in \mathbb{Z}_5\}$. I relativi quozienti sono entrambi isomorfi a $\mathbb{Z}_5$. Basta considerare gli omomorfismi $\varphi_i : A \to \mathbb{Z}_5$, $i = 1, 2$ dati da $\varphi_1([f]) = f(0)$ e $\varphi_2([f]) = f(2)$, mostrare che sono ben definiti e usare primo e terzo teorema di omomorfismo.

Es. 3.10 Abbiamo

$$(S) = \{a_1 s_1 + \cdots + a_k s_k + s_{k+1} + \cdots + s_n : 0 \leq k \leq n,\, a_1 \in A,\, s_j \in S\}.$$

Es. 3.11 Ogni elemento di A è rappresentato da un polinomio di grado al più 1. Gli elementi invertibili sono quelli che non sono multipli né di X né di $X-1$ e quindi sono quelli della forma richiesta. L'unicitá dei coefficienti a e b deriva dal fatto che la differenza tra due polinomi di stinti di grado al pi 'u 1 non puó essere un multiplo di $X^2 - X$.

Es. 3.12 Osservando che $X^2 = X$ abbiamo

$$\begin{aligned}(bX-1)^n &= \sum_{k=0}^{n} \binom{n}{k} b^k X^k (-1)^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} b^k X (-1)^{n-k} - (-1)^n X + (-1)^n \\ &= ((b-1)^n - (-1)^n)X + (-1)^n.\end{aligned}$$

Es. 3.13 Sia ora $f \in A$ tale che $f^n = 1$ si ha chiaramente $f \in U(A)$ e quindi esistono unici $a, b \in \mathbb{C}$ con $b \neq 1$ e $a \neq 0$ tali che $f = a(bX - 1)$. Dal punto precedente abbiamo che $f^n = 1$ se e solo se $(b-1)^n - (-1)^n = 0$ e $(-a)^n = 1$. Abbiamo quindi n scelte (distinte) per a e n scelte (distinte) per b, da cui il risultato. In alternativa si può procedere nel seguente modo. Consideriamo l'omomorfismo

$$\varphi : \mathbb{C}[X] \to \mathbb{C} \times \mathbb{C}$$

dato da $\varphi(f) = (f(0), f(1))$. Questo è suriettivo e il nucleo è proprio $(X^2 - X)$. Per il primo teorema di omomorfismo $A = \mathbb{C} \times \mathbb{C}$ e quindi abbiamo esattamente n^2 elementi che al quadrato danno 1.

. Soluzioni: Teorema cinese del resto ed estensioni quadratiche

Es. 4.1 (a) Abbiamo l'identità di Bézout $13 \cdot 25 - 2 \cdot 162 = 1$ da cui la soluzione è

$$k = 7 \cdot (-2 \cdot 162) + 33 \cdot (13 \cdot 25) = -2268 + 10725 = 8457$$

che è unica modulo $162 \cdot 25 = 4050$. La più piccola soluzione positiva è quindi $8457 - 2 \cdot 4050 = 357$.

Es. 4.2 Procedendo come nell'esercizio precedente (o a occhio) le prime due equazioni sono equivalenti a $k \equiv 16 \mod 35$. Procedendo ancora in modo analogo otteniamo che la soluzione è $k \equiv 401 \mod 420$.

Es. 4.3 Fattorizziamo $1635 = 3 \cdot 5 \cdot 109$. Per il teorema cinese del resto abbiamo che x é soluzione modulo 1635 se e solo se lo é sia modulo 3 che modulo5 che modulo 109.
L'equazione modulo 3 ha come soluzione $x \equiv 1 \mod 3$.
L'equazione modulo 5 ha come soluzione $x \equiv 1, 2 \mod 5$.
Possiamo a questo punto giá dire he le soluzioni modulo 1635 sono esattamente 6, ottenute combinando tutte le possibilitá nei tre moduli. Le soluzioni sono quindi 1 (scegliendo 1,1,1), 7 (scegliendo (1,2,7), 817 (scegliendo 1,2,54) e altre tre...

Es. 4.4 Abbiamo $57 = 3 \cdot 19$ e quindi possiamo risolvere le due equazioni separatamente. L'equazione modulo 3 ha come soluzione $X^2 - 2X \equiv 0 \mod 2$ per cui $X \equiv 0 \mod 2$. Osserviamo che in $\mathbb{Z}_{19}$ l'elemento 2 ha ordine 18 e quindi l'equazione é equivalente a $X^2 - 2X \equiv 0 \mod 18$ che ha come soluzione $X \equiv 0, 2 \mod 18$ (riducendola modulo 2 e modulo 9 si vede facilmente). In conclusione le soluzioni sono quindi $X \equiv 0, 2 \mod 18$.

Es. 4.5 Siano $s \in I$ e $t \in J$ tali che $s + t = 1$. Allora basta scegliere $x = at + bs$. Infatti $x = at + as - as + bs = a - as + bs \equiv a \mod I$ e similmente $x \equiv b \mod J$.

Es. 4.6 Se e solo se d non è un quadrato (dispense).

Es. 4.7 Osservare che $\mathbb{Z}_{(p)}[\sqrt{d}]$ è un sottoanello di $\mathbb{Q}[\sqrt{d}]$. Se quindi d non è quadrato $\mathbb{Z}_{(p)}[\sqrt{d}]$ è un dominio perché sottoanello di un dominio. Se invece $d = a^2 \in \mathbb{Z}_{(p)}$ allora $\mathbb{Z}_{(p)}[\sqrt{d}]$ non è un dominio perché $a + \varepsilon$ è un divisore dello 0.

Es. 4.8 $\mathcal{U}(\mathbb{Z}_{(p)}[\sqrt{p}]) = \{\frac{a}{b} + \varepsilon \frac{c}{d} : p \nmid a,\, p \nmid b,\, p \nmid d\}$.

Es. 4.9 Se $d < 0$ abbiamo $N(a + b\varepsilon) = a^2 - b^2 d$. L'elemento è invertibile se la sua norma lo è e quindi: se $d = -1$ abbiamo ± 1 e $\pm\varepsilon$; se $d < -1$ abbiamo solo ± 1.

Se $d = c^2$ è un quadrato $N(a + b\varepsilon) = a^2 - c^2 b^2 = (a + bc)(a - bc)$. Questo è invertibile, cioè ± 1 se e solo se $a = 0$ e $bc = \pm 1$ oppure $a = \pm 1$ e $bc = 0$. Deduciamo:

- Se $d = 0$ gli invertibili sono $\pm 1 + b\varepsilon$, per ogni $b \in \mathbb{Z}$;
- se $d = 1$ abbiamo $\pm\varepsilon$ e ± 1;
- se $d > 1$ abbiamo ± 1.

Es. 4.10 (a) A è chiaramente un gruppo additivo, contiene 1 ed è chiuso rispetto al prodotto (verifiche comunque da fare)

(b) Infatti se fosse $-1 = (a + 4bi)^2 = a^2 - 16b^2 + 8abi$ per opportuni $a, b \in \mathbb{Z}$ avremmo necessariamente un assurdo.

(c) Basta trovare un elemento non nullo di norma 0 ad esempio $4i + 4\varepsilon$.

Es. 4.11 Se $a + b\varepsilon$ è invertibile allora $a^2 - 2b^2 = \pm 1$. Se $b > a$ avremmo $\pm 1 = a^2 - 2b^2 < b^2 - 2b^2 = -b^2$ assurdo. Se $a \geq 2b$ avremmo $\pm 1 = a^2 - 2b^2 \geq 4b^2 - 2b^2 = 2b^2$ assurdo.

Passo base dell'induzione: Se $b = 1$ e $a + b\varepsilon$ è invertibile (con $a > 0$) abbiamo $a^2 - 2 = \pm 1$ da cui $a = 1$ e quindi $a + b\varepsilon = (1 + \varepsilon)^1$ per cui $(a + \varepsilon b)(-1 + \varepsilon) = (1 + \varepsilon)^1(1 + \varepsilon)^{-1} = (1 + \varepsilon)^0$.

Passo induttivo: supponiamo che l'enunciato sia vero per ogni elemento $(a' + b'\varepsilon)$ invertibile con $a', b' > 0$ e $b' < b$. Calcoliamo

$$(a + \varepsilon b)(-1 + \varepsilon) = -a + 2b + (b - a)\varepsilon;$$

questo elemento soddisfa le ipotesi induttive per cui esiste k tale che

$$(-a + 2b + (b - a)\varepsilon)(-1 + \varepsilon) = (1 + \varepsilon)^k.$$

Ma allora

$$(a + \varepsilon b)(-1 + \varepsilon) = -a + 2b + (b - a)\varepsilon = (1 + \varepsilon)^{k+1}.$$

Sia ora $\alpha = a + b\varepsilon$ invertibile qualunque. Se $a, b > 0$ $\alpha = (1 + \varepsilon)^k$ per quanto visto. Se $a, b < 0$ abbiamo $\alpha = -(1 + \varepsilon)^k$. Se $ab < 0$ allora $\alpha^{-1} = \pm\bar{\alpha}$ e il risultato segue dai casi precedenti. Se $b = 0$ il risultato è banale. $a = 0$ è impossibile.

Es. **??** L'equazione $\omega^2 + \omega + 1 = 0$ segue calcolando esplicitamente le funzioni goniometriche coinvolte $(\cos(\frac{4}{3})\pi = -\frac{1}{2} \cdots)$ oppure osservando che si stanno sommando le tre radici terze dell'unità o anche da $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$. Se $\varphi : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}[\omega]$ abbiamo che necessariamente $\varphi(a + b\varepsilon) = a + b\varphi/\varepsilon$ e inoltre $-3 = \varphi(-3) = \varphi(\varepsilon^2) = (\varphi(\varepsilon))^2$. Bisogna quindi trovare un elemento in $\mathbb{Z}[\omega]$ che al quadrato dia -3. Abbiamo

$$(a + b\omega)^2 = a^2 + b^2\omega^2 + 2ab\omega = a^2 - b^2 + (2ab - b^2)\omega$$

da cui $b(2a - b) = 0$ e $a^2 - b^2 = -3$ che ammette la soluzione $a = 1$, $b = 2$. Abbiamo quindi

$$\phi : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}[\omega]$$

dato da $\phi(a + b\varepsilon) = a + b(1 + 2\omega)$ è un omomorfismo iniettivo e quindi l'immagine è isomorfa a $\mathbb{Z}[\sqrt{-3}]$. L'immagine è propria perché il coefficiente di ω negli elementi dell'immagine è necessariamente pari.

Es. 4.13 Dall'identitá $1 + \omega + \omega^2 = 0$ segue $1 = \omega(-1 - \omega)$ da cui $\omega^{-1} = -1 - \omega \in \mathbb{Z}[\omega]$.

Es. 4.14 La prima parte segue osservando che $\bar{\alpha} = a + b\bar{\omega} = a + b\omega^2$ e facendo il conto. La seconda parte segue dalla moltiplicativitá delle norme (osservando che le norme sono sempre interi non negativi) e che se $N(\alpha) = 1$ allora $\bar{\alpha} = \alpha^{-1}$.

Es. 4.16 L'ideale $(2, \varepsilon)$ è proprio. Se fosse principale sarebbe generato da un divisore non invertibile di 2, quindi da un elemento di norma 4 e quindi del tipo $2 + b\varepsilon$. Consideriamo l'ideale principale $J = (2 + b\varepsilon)$: esso contiene gli elementi della forma $(2 + b\varepsilon)(a + c\varepsilon) = 2a + (ab + 2c)\varepsilon$ al variare di $a, c \in \mathbb{Z}$. Osserviamo quindi che $\varepsilon \notin J$ e il risultato segue. La seconda parte è ovvia perché ε è invertibile.

Es. 4.17 Per trovare un isomorfismo dobbiamo trovare in $\mathbb{Z}[\sqrt{3}]$ un elemento che al quadrato dia 2. Questo è $2\sqrt{3}$ e quindi basta mostrare che

$$\varphi : \mathbb{Z}_5[\sqrt{2}] \to \mathbb{Z}_5[\sqrt{3}]$$

dato da $\varphi(a + b\sqrt{2}) = a + b(2\sqrt{3})$ è un omomorfismo (biunivoco).

. Soluzioni: Primi, irriducibili, domini euclidei

Es. 5.1 In $\mathbb{Z}_5$: 2, in $\mathbb{Z}_{13}$: 5, in $\mathbb{Z}_{17}$: 4, in $\mathbb{Z}_3[\sqrt{2}]$: ε, in $\mathbb{Z}_7[\sqrt{3}]$: 3ε, in $\mathbb{Z}_{11}[\sqrt{2}]$: 4ε.

Es. 5.2 $a+b$ e $a'+b'$ in generale non sono associati (cerca un controesempio); ab e $a'b'$ lo sono sempre.

Es. 5.3 Ogni elemento non nullo è associato a 1 e quindi è invertibile.

Es. 5.4 $(5, 3+4i)$: nessuno dei due divide l'altro perché hanno la stessa norma e non sono associati;
$(3+i, 2+4i)$: il primo ha norma 10 il secondo 20. Si ha $(2+4i)(3+i)^{-1} = 1+i$ quindi $3+i|2+4i$.
$(5+i, 5-i)$: hanno stessa norma, ma non sono associati, come nel primo punto;
$(17+i, 13+7i)$: le norme (290 e 218) non si dividono, quindi neanche gli elementi.

Es. 5.5 Consideriamo $1+d = (1+\varepsilon)(1-\varepsilon)$. Siccome d é dispari abbiamo $2|(1+\varepsilon)(1-\varepsilon)$ e inoltre 2 non divide nessuno dei due fattori (perché non hanno coefficienti pari) e quindi sicuramente 2 non é primo. Tuttavia se 2 non fosse irriducibile sarebbe il prodotto di due elementi di norma 2. Ma $N(a+\varepsilon b) = a^2 + db^2$ é sempre diversa da 2.

Es. 5.6 Simile al precedente. Siccome $d+1$ non é primo abbiamo che esiste un primo p che divide propriamente $d+1$. Siccome $d+1 = 1+\varepsilon)(1-\varepsilon)$ abbiamo che p non puó essere primo in $\mathbb{Z}[\sqrt{-d}]$. Se p fosse riducibile esisterebbero $a, b \in \mathbb{Z}$ tali che $a^2 + db^2 = p$. Siccome $p|d$ abbiamo in particolare $p < d$ e quindi abbiamo necessariamente $b = 0$ che porta alla condizione $a^2 = p$, assurdo.

Es. 5.7 Si ha $I = (\alpha)$ se e solo se $\alpha = MCD(3+i, 1+5i)$. Abbiamo $N(3+i) = 10$ e $N(1+5i) = 26$ quindi $MCD(3+i, 1+5i) = 1+i$ (perché?). Abbiamo quindi che i possibili α sono quattro, cioè $\pm 1 \pm i$. Se $N(a)$ è pari allora a è divisibile per $1+i$. Se $N(a)$ è dispari si ha $N(a+1)$ pari e il risultato segue. Da questo segue che $\mathbb{Z}[i]/I$ è un anello con due elementi, e quindi un campo.

Es. 5.8 Se $\alpha \in I$, $\alpha \neq 0$ ogni classe di $\mathbb{Z}[i]/I$ contiene un elemento di norma minore della norma di α (il resto nella sua divisione per α). Siccome gli elementi di norma minore della norma di α sono finiti, anche le classi sono finite.

Es. 5.9 Procedendo come nella dimostrazione per $d = -1, \pm 2$ ci riduciamo a mostrare che se $a, b \in \mathbb{Q}$ sono tali che $|a|, |b| \leq \frac{1}{2}$ allora $|N(a+b\varepsilon)| < 1$ cioè $|a^2 - 3b^2| < 1$; ma questo è evidente perché

$$-1 < -\frac{3}{4} \leq -3b^2 \leq a^2 - 3b^2 \leq a^2 \leq \frac{1}{4} < 1.$$

Es. 5.10 Osserviamo (calcolando) che $\mathbb{Z}[\omega]$ contiene un elemento che al quadrato dà -3: questo è $1+2\omega$. L'omomorfismo che cerchiamo

$$\varphi : \mathbb{Z}[\omega] \to \mathbb{Q}[\sqrt{-3}]$$

dovrà essere tale che $\varphi(1+2\omega) = \varepsilon$. Questo si ottiene ponendo

$$\varphi(a+b\omega) = a - \frac{b}{2} + \frac{b}{2}\varepsilon$$

e si verifica che φ è un omomorfismo iniettivo. Osserviamo che l'immagine isomorfa di $\mathbb{Z}[\omega]$ in $\mathbb{Z}[\sqrt{-3}$ è data da tutti gli elementi della forma $\frac{1}{2}(a+b\varepsilon)$ con a, b entrambi pari o entrambi dispari. Per mostrare che è euclideo procediamo come negli altri casi. Ci si riduce a mostrare che se a, b sono tali che $|a| \leq \frac{1}{4}$ e $|b| \leq \frac{1}{2}$ (o viceversa), allora $a^2 + 3b^2 < 1$.

Es. 5.11 Osservare che entrambe le condizioni sono equivalenti a $N(a + bi)$ pari.

Es. 5.12 Abbiamo $N(8 + i) = 65$ e $N(4 + 13i) = 185$ per cui se $\alpha = MCD(8 + i, 4 + 13i)$ abbiamo $N(\alpha) = 1, 5$. In effetti si può verificare che $1 + 2i$ divide entrambi gli elementi e quindi abbiamo $\alpha = 1 + 2i$. E i multipli di α sono propri gli elementi della forma $c - 2d + i(2c + d)$ e ponendo $c - 2d = a$ abbiamo gli elementi della forma $a + i(2a + 5d)$, cioè gli elementi $a + ib$ tali che $2a \equiv b \mod 5$ o equivalentemente $a \equiv 3b \mod 5$. Ogni elemento $a+ib$ è quindi equivalente a $a+ib+(-3b-ib) = a-3b$. Osserviamo infine che i numeri interi 1,2,3,4 sono tutti non nulli mentre $5 = 0$ e quindi concludiamo. In alternativa si può considerare l'omomorfismo

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5$$

dato da $\varphi(a+ib) = a-3b$, mostrare che è un omomorfismo e che il nucleo è proprio I.

Es. 5.13 Supponiamo che $\rho(a - b) \leq \max\{\rho(a), \rho(b)\}$ per ogni $a, b \in A$. Siano $\alpha, \beta \in A$ con $\beta \neq 0$ e supponiamo $\alpha = q_1\beta + r_1 = q_2\beta + r_2$, e quindi $(q_1 - q_2)\beta = r_2 - r_1$, con $\rho(r_1), \rho(r_2) < \rho(\beta)$. Allora, se $q_1 \neq q_2$,

$$\rho(\beta) \leq \rho((q_1 - q_2)\beta) = \rho(r_2 - r_1) \leq \rho(r_1) < \rho(\beta).$$

Viceversa, se esistono $a, b \in A$ tali che $\rho(a - b) > \max(\rho(a), \rho(b))$ allora abbiamo due modi diversi di dividere a per $a - b$:

$$a = 1 \cdot (a - b) + b, \quad a = 0 \cdot (a - b) + a.$$

. Soluzioni: MCD

Es. 6.1 $(5, 3+4i)$: sappiamo che $5 = \pi_5\bar{\pi}_5$ e quindi abbiamo che $3+4i = \pi_5^2$ oppure $\bar{\pi}_5^2$ a meno di associati. In effetti $\pi_5^2 = (1+2i)^2 = -3+4i$ che non è associato a $3+4i$ e quindi $3+4i$ è associato a $\bar{\pi}_5^2$ e quindi

$$MCD(5, 3+4i) = \bar{\pi}_5 = 1-2i.$$

$(3+i, 2+4i)$: abbiamo già visto che $3+i$ divide $2+4i$ per cui $MCD(3+i, 2+4i) = 3+i$.

Es. 6.2 $(5+i, 5-i)$: essendo coniugati, di norma dispari e non essendo divisi da alcun numero primo p necessariamente $MCD(5+i, 5-i) = 1$.
$(17+i, 13+7i)$: guardando le norme :$290 = 2\cdot 5\cdot 29$ e $218 = 2\cdot 109$ l'unica possibilità è $MCD(17+i, 13+7i) = 1+i$.

Es. 6.3 Siccome $N(p) = p^2$ abbiamo che p è riducibile se e solo se esistono α, β di norma p tali che $\alpha \cdot \beta = p$. Questo è equivalente all'esistenza di α di norma p: infatti in tal caso basta scegliere $\beta = \bar{\alpha}$. Il risultato segue.

Es. 6.4 Segue dalla moltiplicatività della norma e dal fatto che gli elementi invertibili sono quelli di norma 1.
Cerchiamo gli elementi irriducibli di norma al più 10.
Norma 2: $\pm\sqrt{-2}$.
Norma 3: $\pm 1 \pm \sqrt{-2}$ sono irriducibili perché hanno norma prima.
Norma 4: ± 2 sono riducibili
Norma 5: non ci sono
Norma 6: $\pm 2 \pm \sqrt{-2}$: sono riducibili perché sono i prodotti degli elementi di norma 2 e quelli di norma 3.
Norma 7: non ci sono
Norma 8: $\pm 2\sqrt{-2}$ sono chiaramente riducibili
Norma 9: ± 3 sono riducibili
Norma 10: non ci sono.

Es. 6.5 Per $p = 2$ il risultato è banale. Se p è dispari abbiamo $a^2 = -1$ implica $(2a)^2 = -4$ e viceversa, $b^2 = -4$ implica $(b2^{-1})^2 = -1$ e quindi -4 è un quadrato se e solo se -1 lo è. Il risultato segue quindi dal risultato noto per -1.

Es. 6.6
- 2 é irriducibile perché non esistono elementi di norma 2. Tuttavia 2 non é primo perché é un divisore di ε^2 ma non di ε.
- se $p \equiv 1 \mod 4$ allora -4 è un quadrato in $\mathbb{Z}_p$ e quindi esiste $a, k \in \mathbb{Z}$ tale che $a^2 = -4 + kp$ per l'esercizio precedente. Da questo segue che $a^2 + 4 = kp$ e quindi $(a+\sqrt{-4})(a-\sqrt{-4}) = kp$. Se p fosse primo avremmo $p|(a+\sqrt{-4})$ oppure $p|(a-\sqrt{-4})$ entrambi i casi sono assurdi perché p non divide il coefficiente di $\sqrt{-4}$. Osserviamo inoltre che p non é neanche irriducibile in quanto sappiamo che p é somma di due quadrati ed uno di questi é pari $p = a^2 + (2b)^2$ e quindi esistono elementi di norma p.
- se $p \equiv 3 \mod 4$. Supponiamo $p|(a+\sqrt{-4}b)(c+\sqrt{-4}d)$. Da questo segue, per la moltiplicatività delle norme, che $p^2|(a^2+4b^2)(c^2+4d^2)$ Siccome p é un

numero primo possiamo quindi assumere che $p|a^2+4b^2$. Ma allora $a^2=-4b^2 \mod p$. Se $p|b$ allora $p|a$ e quindi $p|a+\sqrt{-4}b$. Altrimenti abbiamo che b è invertibile $modp$ e quindi avremmo $-4=(ab^{-1})^2 \mod p$, un assurdo per l'esercizio precedente.
In alternativa si puó sfruttare il fatto che $\mathbb{Z}[\sqrt{-4}]$ é un sottoanello di $\mathbb{Z}[i]$ (tramite l'omomorfismo $(a+b\sqrt{-4}\mapsto a+2bi)$: sappiamo che p é primo in $\mathbb{Z}[i]$ per cui $p|a+2bi$ in $\mathbb{Z}[i]$ e quindi sia a che b sono multipli di 4.

Es. 6.7 La norma di un elemento $a+b\varepsilon$ in $\mathbb{Z}[\sqrt{-6}]$ è a^2+6b^2 e quindi non esistono elementi di norma 2 né di norma 5. Di conseguenza 2 e 5 sono irriducibili. Ma 2 non è primo perché 2 divide $\varepsilon^2=-6$ ma non divide ε. Analogamente 5 non è primo perché divide $10=(2+\varepsilon)(2-\varepsilon)$ ma non divide nessuno dei due fattori.

Es. 6.8 $N(10)=100$ e $N(4+2\varepsilon)=40$ quindi se d è un MCD si deve avere $N(d)|20$. Inoltre 2 e $2+\varepsilon$ sono divisori comuni di 10 e di $4+2\varepsilon$ e quindi le loro norme devono dividere $N(d)$. Ma le loro norme sono 4 e 10 e quindi deduciamo $N(d)=20$ che è assurdo.

Es. 6.9 Siccome A è euclideo abbiamo $I=(\alpha)$. Un ideale che contiene I deve essere generato da un divisore di α, e questi sono finiti perché A è UFD.

Es. 6.10 $0\in I$. Se $x,y\in I$ allora $x\in I_j$, $y\in I_k$. Se $j\le k$ allora $x,y\in I_k$ e quindi $x-y\in I_k\subset I$. Se $a\in A$ abbiamo $ax\in I_j\subset I$.

Es. 6.11 Il fatto che A sia un dominio è una verifica di routine. Ponendo $I_j=(x_jx_{j+1}\cdots)$ abbiamo evidentemente che $I_1\subset I_2\subset I_3\cdots$, con le inclusioni tutte strette perché $x_jx_{j+1}\cdots\notin I_{j-1}$.

Es. 6.12 È sufficiente mostrare che se un "monomio infinito" M si scrive come prodotto di due elementi f,g di A, $M=fg$ allora f e g sono anch'essi monomi (di cui almeno uno infinito). Infatti, in tal caso in ogni fattorizzazione di un monomio infinito avremmo sempre almeno un monomio infinito che evidentemente non è irriducibile.

Mostriamo ora che se $M=fg$ allora f e g sono monomi. Supponiamo per assurdo che f non sia un monomio e che quindi sia combinazione lineare di almeno due monomi. Introduciamo un ordinamento totale tra i monomi: sia $M=x_1^{m_1}x_2^{m_2}\cdots$ e $N=x_1^{n_1}x_2^{n_2}\cdots$. Diciamo che $M<N$ se, posto $k=\min\{i : m_i\neq n_i\}$ si ha $m_i<n_i$. In altre parole il primo esponente di M diverso da quello corrispondente di N deve essere più piccolo. Chiamiamo M_1 il monomio più grande che compare in f M_2 il più piccolo che compare in f, N_1 il più grande che compare in g e N_2 il più piccolo che compare in g. Se f non è un monomio si ha $M_1\neq M_2$ e si può verificare che M_1N_1 e M_2N_2 sono due monomi distinti che compaiono in fg con coefficienti non nulli e quindi fg non può essere un monomio.

Es. 6.13 $5+6i=\pi_{61}$
$24=2^4\cdot 3$ e quindi è associato a $(1+i)^63$. Più precisamente si ha $24=-i(1+i)^63$.
$6+4i=(1+i)^2\bar{\pi}_{13}$.

Es. 6.14 La prima parte é una semplice verifica. Consideriamo ora la norma complessa di un elemento di questo anello: abbiamo $N(a+b\eta)=(a+\frac{b}{2})^2+\frac{19}{4}b^2)$ per cui tutti gli elementi con $b\neq 0$ hanno norma maggiore di 4 e quelli con $b=0$ hanno norma a^2 che é sempre almeno 1 tranne se $a=0$. Gli elementi invertibili sono quindi solo

± 1. Il fatto che 2 e 3 siano irriducibili segue ancora da quanto detto prima sulle possibili norme degli elementi di questo anello. Sia α un elemento che minimizza la ρ tra i ninz. Allora nella divisione euclidea di 2 per α otteniamo $2 = q\alpha + r$ dove per minimalitá otteniamo $r = 0, \pm 1$. Se $r = 0$ otteniamo $2 = q\alpha$ da cui per irriducibilitá di 2 abbiamo α associato a 2. Se $r = -1$ analogamente otteniamo $3 = q\alpha$ da cui α é associato a 3. Infine, se $r = 1$ otteniamo $1 = q\alpha$, assurdo perché α é ninz. L'ultima parte segue osservando che se $\alpha = \pm 2, \pm 3$ e $r = 0, \pm 1$ allora non si puó avere $\eta = q\alpha + r$.

Es. 6.15 Sia $d = MCD_A(a_1, a_2)$. Siccome A é un PID abbiamo $(d) = (a_1, a_2)$ e quindi esistono $x, y \in A$ tali che $d = xa_1 + ya_2$. Allora d soddisfa la definizione di MCD tra a_1 e a_2 anche in B.