Algebra 2
Esercizi 10 - 28 dicembre 2022

Alcuni suggerimenti per i seguenti esercizi si trovano in fondo al testo.

Gruppi, teoremi di Sylow

1. Sia G un gruppo finito di ordine n e H un sottogruppo di G di indice 2 (cioè H è di ordine $n/2$). Provare che H è normale in G.

2. Sia G un gruppo tale che $g^2 = 1$ per ogni $g \in G$. Provare che G è abeliano.

3. Sia $\phi : G_1 \longrightarrow G_2$ un monomorfismo di gruppi. Provare che se G_2 è abeliano, anche G_1 lo è. Dare un esempio per provare che l'ipotesi che ϕ sia monomorfismo è essenziale.

4. Sia G un gruppo finito di ordine 325. Ci sono due sottogruppi normali non banali in G?

5. Si consideri la seguente matrice:

$$\begin{pmatrix} \sqrt{3}/2 & -1/2 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}$$

   Sia $G = \{A^i \mid i \in \mathbb{Z}\}$. Che ordine ha il gruppo G? Si riesce a dare un significato geometrico al gruppo G?

Anelli, ideali

6. Provare che per ogni $n \in \mathbb{Z}$ non divisibile per 7, il numero $3n^{12}+n^7+6n+4$ è divisibile per 7.

7. Sia A un anello che soddisfa la condizione:

$$\text{per ogni } a \in A \text{ esiste } n \in \mathbb{N},\ n > 1, \text{ tale che } a^n = a$$

   Provare allora che in A ogni ideale primo è anche massimale.

8. Sia K un campo. Trovare tutti gli ideali dell'anello $K \times K$.

9. Provare che l'anello $\mathbb{Z}_6 \times \mathbb{Z}_6$ non è isomorfo a $\mathbb{Z}_{36}$.

10. Sia $A = \mathbb{Z}_4[x]/(x^2)$. Quanti elementi ha l'anello A? Indicare tutti gli elementi di A che sono invertibili.

11. Dare l'esempio di un anello, di caratteristica 6 che ha infiniti elementi.

12. Sia A un anello di cartteristica 6. Provare che A non può avere 7 elementi. Più in generale, provare che un anello di caratteristica $n \in \mathbb{N}$ non può avere $n + 1$ elementi.

13. Dare l'esempio di un anello A di caratteristica 6 tale che il suo quoziente A/I fatto rispetto ad un suo ideale I è un anello che non ha caratteristica 6.

Anello di polinomi in una variabile

14. Sia K un campo, $a \in K$ un elemento non nullo fissato e si consideri l'omomorfismo $\phi : K[x] \longrightarrow K[x]$ tale che $\phi(x) = ax$ (e $\phi(u) = u$ per ogni $u \in K$). Provare che ϕ è un isomorfismo di anelli.

15. Sia $a \in \mathbb{N}$ un numero con fattorizzazione in numeri primi data da: $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Provare che se almeno un esponente α_i vale 1, allora il polinomio

$$x^n + ax^2 + a \in \mathbb{Z}[x]$$

è irriducibile (per ogni $n \geq 3$).

16. Sia $f(x) = x^3 + 3ax + 2b \in \mathbb{C}[x]$. Per quali valori di a e b il polinomio non ha radici distinte?

17. Dire quanti fattori irriducibili ha il polinomio $x^{108} + 1 \in \mathbb{Z}_3[x]$.

18. Usando l'algoritmo di Berlekamp, trovare la fattorizzazione, in fattori irriducibili, di $x^4 + 1 \in \mathbb{Z}_5[x]$.

Ideali di $K[x_1, \dots, x_n]$

19. Si consideri l'ideale $I = (x + 3, y^2 + 4) \subseteq \mathbb{Z}_5[x, y]$. Trovare tutti gli ideali massimali che contengono I.

20. Sia $I = (x^3, y^3 - y) \subseteq K[x, y]$ (dove K è un campo). Trovare tutti gli ideali primi che contengono I. Provare poi che questi ideali primi sono anche massimali.

Estensioni di campi, elementi algebrici

21. Sia $a \in \mathbb{C}$ e supponiamo che $a \in \mathbb{Q}[a^3]$. Provare che a è algebrico su $\mathbb{Q}$.

22. Siano K ed L campi, con L estensione di K. Sia poi $a \in L$ algebrico su K, di grado n (cioè il suo polinomio minimo su K è di grado n). Provare che $10a$ è algebrico su K. Che grado ha $10a$ su K?

23. Sia $f = x^3 + 2x^2 - 3 \in \mathbb{Q}[x]$. Trovare un campo di riducibilità completa di f.

24.* Provare che $a = \sqrt{3 + 2\sqrt{2}}$ è algebrico su $\mathbb{Q}$. Trovare il suo polinomio minimo.

25.* Provare che $\sqrt[3]{2} + \sqrt[3]{4}$ è algebrico su $\mathbb{Q}$. Trovare il suo polinomio minimo.

26. Sia $a \in \mathbb{C}$ algebrico su $\mathbb{Q}$. Provare che $a^2 + 1$ è algebrico su $\mathbb{Q}$.

Campi finiti

27. Sia $(K = \{0, 1, 2, 3\}, +, \cdot)$ un insieme con due operazioni definite dalle seguenti tabelle:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

K risulta un campo. Pertanto deve essere della forma $\mathbb{Z}_p[x]/(q)$ dove p è un numero primo e q è un polinomio irriducibile. Trovare p e q e l'isomorfismo tra K e $\mathbb{Z}_p[x]/(q)$.

28. Provare che $\mathbb{Z}_3[x]/(x^2 + 1)$ è un campo e trovare tutti i suoi elementi primitivi.

29. Sia L un campo finito con 49 elementi e si supponga che L sia un'estensione di un campo K. Cosa si può dire di K?

Suggerimenti per le soluzioni

Esercizio 1 Quanti sono i laterali gH con $g \in G$ e i laterali Hg con $g \in G$? Si può dedurre che i laterali destri e sinistri conicidono?

Esercizio 2 Si tratta di vedere che $gh = hg$ per ogni g e h. Ma g^2, h^2 e $(gh)^2 = ghgh$ valgono 1. Quindi $ghgh = 1$ e si provi a moltilpicare a sinistra per g ...

Esercizio 3 Si tratta di vedere che $gh = hg$. Si applichi ϕ e si usi l'iniettività.

Esercizio 4 Usare i teoremi di Sylow e calcolare N_5 e N_{13}.

Esercizio 5 Pensare alla matrice $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$.

Esercizio 6 Il piccolo teorema di Fermat dice che, se 7 non divide n, allora $n^6 \equiv 1 \mod 7$.

Esercizio 7 Basta provare che se $\mathcal{P}$ è primo, allora il quoziente $A/\mathcal{P}$ è un campo. Se $[a] \neq 0$ in $A/\mathcal{P}$, allora $a(a^{n-1} - 1) \in \mathcal{P}$ allora ...

Esercizio 8 Se I è un ideale di $K \times K$, allora $p_1(I)$ è un ideale di K, dove $p_1 : K \times K \longrightarrow K$ è la proiezione sul primo fattore...

Esercizio 9 Che ordini hanno gli elementi di $\mathbb{Z}_6 \times \mathbb{Z}_6$? E che ordini possono avere gli elementi di $\mathbb{Z}_{36}$?

Esercizio 10 Un elemento di A 'e una classe del tipo $[a_0+a_1x+a_2x^2+a_3x^3+\cdots]$ ma in A $[x^2]=0$, quindi ...

Esercizio 11 Ricordare che un anello di polinomi ha infiniti elementi. Inoltre, se A è un anello di caratteristica c, l'anello dei polinomi $A[x]$ ha ancora caratteristica c.

Esercizio 12 L'anello A contiene (una copia isomorfa di) $\mathbb{Z}_6$ e un ulteriore elemento a. Quanto fa $a+1$?

Esercizio 13 Forse l'anello $\mathbb{Z}_6$ può aiutare.

Esercizio 14 Si riesce a trovare una $\psi : K[x] \longrightarrow K[x]$ che sia inversa di ϕ? Dove deve mandare le costanti ψ? E dove deve mandare la x?

Esercizio 15 Forse Eisenstein può aiutare...

Esercizio 16 Un modo di procedere potrebbe essere quello di vedere quando un polinomio ha fattori multipli (usando il suo derivato...)

Esercizio 17 Ricordare che $a^p+b^p=(a+b)^p$ in caratteristica p e ricordare che Berlekamp permette di capire quanti fattori irriducibili ha un polinomio.

Esercizio 18 Ogni tanto nella vita va fatto un esempio di fattorizzazione con Berlekamp.

Esercizio 19 Il polinomio y^2+4 si fattorizza? Ricordare che un ideale massimale in particolare è un ideale primo e ricordare che ideali della forma $(x-a, y-b)$ in $K[x,y]$ sono massimali ...

Esercizio 20 Simile al precedente.

Esercizio 21 Se $a \in \mathbb{Q}[a^3]$, come può essere scritto a? Altro modo per procedere: usare il teorema della torre.

Esercizio 22 Considerare $[K[a] : K]$ e $[K[10a] : K]$. Quando si può dire che $K[a] = K[10a]$? Attenzione alla caratteristica...

Esercizio 23 Adattare la dimostrazione generale a questo caso.

Esercizio 24 Non è che forse $3+2\sqrt{2}$ è un quadrato?

Esercizio 25 Detto $a = \sqrt[3]{2} + \sqrt[3]{4}$, non è che forse che a^3 si può scrivere come un polinomio in a? Per il polimonio minimo, potrebbe essere utile usare opportunamente Eisenstein.

Esercizio 26 Un modo per risolverlo è di far ricorso al teorema della torre.

Esercizio 27 Prima di tutto, dalla tabella della somma, si dovrebbe trovare facilmente la caratteristrica p di K. Successivamente, si tratta di trovare un polinomio irriducibile di $\mathbb{Z}_p[x]$ di grado n in modo che $p^n =?$

Esercizio 28 Il quoziente è un campo se e solo se l'ideale $(x^2 + 1)$ è... . Per gli elementi primitivi, scrivere ad uno ad uno gli elementi del campo.

Esercizio 29 Usare opportunamente il teorema della torre per vedere tutte le possibilità che può avere K.