

### 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  $\phi : G_1 \rightarrow G_2$  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  $\phi$  sia monomorfismo è essenziale.
4. Sia  $G$  un gruppo finito di ordine 325. Quanti sottogruppi normali ha  $G$ ?
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  $G$ ?

6. Sia  $C_2 = \{1, a\}$  un gruppo ciclico di ordine 2 (quindi  $a^2 = 1$ ) e sia  $G = S_3 \times C_2$ . Trovare tutti i sottogruppi di Sylow di  $G$  e verificare che il loro numero è coerente con quanto affermato dai teoremi di Sylow.

### Anelli, ideali

1. Provare che per ogni  $n \in \mathbb{Z}$ , il numero  $3n^{12} + n^7 + 6n + 4$  è divisibile per 7.
2. Sia  $A$  un anello che soddisfa la condizione:  
per ogni  $a \in A$  esiste  $n \in \mathbb{N}$ ,  $n > 1$ , tale che  $a^n = a$   
Provare allora che in  $A$  ogni ideale primo è anche massimale.
3. Sia  $K$  un campo. Trovare tutti gli ideali dell'anello  $K \times K$ .
4. Provare che l'anello  $\mathbb{Z}_6 \times \mathbb{Z}_6$  non è isomorfo a  $\mathbb{Z}_{36}$ .
5. Sia  $A = \mathbb{Z}_4[x]/(x^2)$ . Quanti elementi ha l'anello  $A$ ? Indicare tutti gli elementi di  $A$  che sono invertibili.
6. Dare l'esempio di un anello, di caratteristica 6 che ha infiniti elementi. Provare poi che non esistono anelli di caratteristica 6 con 7 elementi.
7. 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

1. Sia  $K$  un campo,  $a \in K$  un elemento non nullo fissato e si consideri l'omomorfismo  $\phi : K[x] \rightarrow K[x]$  tale che  $\phi(x) = ax$  (e  $\phi(u) = u$  per ogni  $u \in K$ ). Provare che  $\phi$  è un isomorfismo di anelli.
2. 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  $\alpha_i$  vale 1, allora il polinomio

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

è irriducibile (per ogni  $n \geq 3$ ).

3. Sia  $f(x) = x^3 + 3ax + 2b \in \mathbb{C}[x]$ . Per quali valori di  $a$  e  $b$  il polinomio non ha radici distinte?
4. Dire quanti fattori irriducibili ha il polinomio  $x^{108} + 1 \in \mathbb{Z}_3[x]$ .
5. Usando l'algoritmo di Berlekamp, trovare la fattorizzazione, in fattori irriducibili, di  $x^4 + 1 \in \mathbb{Z}_5[x]$ .

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

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

1. Sia  $a \in \mathbb{C}$  e supponiamo che  $a \in \mathbb{Q}[a^3]$ . Provare che  $a$  è algebrico su  $\mathbb{Q}$ .
2. 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  $K$ ?
3. Sia  $f = x^3 + 2x^2 - 3 \in \mathbb{Q}[x]$ . Trovare un campo di riducibilità completa di  $f$ .
- 4.\* Provare che  $a = \sqrt{3 + 2\sqrt{2}}$  è algebrico su  $\mathbb{Q}$ . Trovare il suo polinomio minimo.
- 5.\* Provare che  $\sqrt[3]{2} + \sqrt[3]{4}$  è algebrico su  $\mathbb{Q}$ . Trovare il suo polinomio minimo.
6. Sia  $a \in \mathbb{C}$  algebrico su  $\mathbb{Q}$ . Provare che  $a^2 + 1$  è algebrico su  $\mathbb{Q}$ .

### Campi finiti

1. 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

·	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  $\mathbb{Z}_p[x]/(q)$ .

2. Provare che  $\mathbb{Z}_3[x]/(x^2 + 1)$  è un campo e trovare tutti i suoi elementi primitivi.
3. 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  $K$ ?
4. Ripercorrendo la dimostrazione relativa al teorema dell'elemento primitivo, provare che se  $K$  è un campo e se  $G$  è un sottogruppo finito del gruppo moltiplicativo  $K \setminus \{0\}$ , allora  $G$  è ciclico.