Prove di esame e altri esercizi di Algebra 1997-99

Esercizi vari

1) Sia X un insieme, e sia $\mathcal{P}(X)$ l'insieme dei suoi sottinsiemi. Se A e B sono sottinsiemi di X, poniamo

$$A \odot B = A \cup B - A \cap B\,.$$

a) Mostrare che l'operazione $\odot$ è associativa, cioè che, dati comunque tre sottinsiemi A, B e C di X, si ha che

$$(A \odot B) \odot C = A \odot (B \odot C)\,.$$

b) Mostrare che $\mathcal{P}(X)$, con l'operazione $\odot$, è un gruppo abeliano.

2) Sia G un gruppo non abeliano e sia H l'insieme dei suoi elementi di ordine finito. VERO O FALSO: se H è un sottogruppo di G allora è un sottogruppo normale.

3) Siano H e K gruppi ciclici finiti. Sia G il gruppo $H \times K$, con il prodotto

$$(h,k)(h',k') = (hh',kk')\,.$$

Mostrare che, se gli ordini di H e K sono primi fra loro, allora G è ciclico, e che un suo generatore è (a,b), dove a è un genereatore di H e b uno di K.

Prova scritta del 8 gennaio 1997

4) Dire se la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 8 & 9 & 2 & 7 & 4 & 3 & 6 & 10 \end{pmatrix}$$

è pari o dispari.

5) Date le applicazioni α e β di $\mathbb{N}$ in $\mathbb{N}$ definite da

$$\alpha(x) = x^2 + 1\,, \quad \beta(x) = 3x + 2\,,$$

calcolare $\alpha \circ \beta$, $\beta \circ \alpha$, α^2, β^2.

6) a) Quante sono le applicazioni iniettive di un insieme di 5 elementi in uno di 8?
b) In generale, dati due insiemi finiti X e Y aventi, rispettivamente, h e k elementi, quante sono le applicazioni iniettive di X in Y?

7) Sia X un insieme non vuoto, e sia F l'insieme di tutte le applicazioni di X in sè. Dire in quali casi F, con l'operazione di composizione di applicazioni, è un gruppo. In generale dire quali degli assiomi di gruppo sono soddisfatti da F.

8) Sia G un gruppo, e siano x e y due suoi elementi di ordini finiti h e k.
   a) Si mostri che, se G è abeliano e h e k sono primi fra loro, allora l'ordine di xy è esattamente hk.
   b) Si mostri che la conclusione di a) non è necessariamente vera se G non è abeliano.
   c) Si mostri che, se G è abeliano, allora l'ordine di xy divide hk/m ed è diviso da hk/m^2, dove m è il massimo comun divisore di h e k.

Prova scritta del 29 gennaio 1997

9) Sia X un insieme finito con n elementi. Mostrare che i sottinsiemi di X con un numero pari di elementi sono 2^{n-1} (Suggerimento: ragionare per induzione su n).

10) Sia G un gruppo abeliano di ordine finito dispari e sia φ un suo automorfismo. Si ponga $H = \{g \in G : \varphi(g) = g\}$, $K = \{g \in G : \varphi(g) = g^{-1}\}$. Si mostri che H e K sono sottogruppi di G e che $H \cap K = \{\mathbf{1}\}$.

11) Sia G un gruppo; per ogni intero positivo n poniamo $G_n = \{g \in G : g^n = \mathbf{1}\}$.
   a) Si mostri che, se G è abeliano, allora G_n è un sottogruppo di G.
   b) Si mostri che, se G non è abeliano, G_n può non essere un sottogruppo di G.
   c) Si mostri che, se G_n è un sottogruppo di G, è un sottogruppo normale.

12) Sia G un gruppo ciclico, e siano H e K due suoi sottogruppi, di ordini 20 e 84.
   a) Il gruppo G può essere infinito?
   b) Nel caso in cui G sia finito, cosa si può dire sul suo ordine?
   c) Qual'è l'ordine di $H \cap K$?

Prova scritta del 21 aprile 1997

13) Siano G e K gruppi e sia $\alpha : G \to K$ un omomorfismo suriettivo. Si supponga che G abbia un sistema di generatori finito. Si dimostri che anche K ha un sistema di generatori finito.

14) Sia p un numero primo e sia n un intero positivo. Trovare un gruppo finito G e due sottogruppi di G di ordine p^n che non siano coniugati.

15) Sia G un gruppo di ordine $5 \cdot 13 \cdot 17$. Dimostrare che G è abeliano.

16) Siano G e K due gruppi, e sia $\alpha : G \to K$ un omomorfismo suriettivo. Sia H un sottogruppo di K; si mostri che H è normale se e solo se $\alpha^{-1}(H)$ è normale in G.

Prova scritta del 27 maggio 1997

17) Sia G un gruppo di ordine 99. Si mostri che G è abeliano (suggerimento: usare i teoremi di Sylow).

18) Dimostrare che un gruppo infinito ha sempre infiniti sottogruppi.

19) Sia K il campo $\mathbb{Z}/(3)$ e si consideri il polinomio $p(X) = X^3 + X^2 + X + 1 \in K[X]$. Sia I l'ideale in $K[X]$ generato da $p(X)$.
   a) Si mostri che $A = K[X]/I$ non è un campo.
   b) Trovare i divisori di zero e gli elementi invertibili di A.
   c) Calcolare, se esiste, l'inverso della classe di X in A.

20) In $\mathbb{Q}[X]$ trovare il generatore monico $p(X)$ dell'ideale I generato dai due polinomi

$$f(X) = X^4 - X^3 + 2X^2 - 2X\,,$$
$$g(X) = 2X^3 - 2X^2 + 3X - 3\,.$$

   Dire se I è primo e se è massimale.

21) Sia p un numero primo. Sia R l'insieme di tutti i numeri razionali della forma a/p^n, dove a è un intero e n è un intero non negativo.
   a) Mostrare che R è un sottoanello di $\mathbb{Q}$.
   b) Mostrare che ogni ideale di R è principale.
   c) Descrivere tutti gli ideali massimali di R.

Prova scritta del 24 giugno 1997

22) Costruire, in S_4, il sottogruppo G generato dai tre elementi

$$\alpha = (1\ 2)\,, \quad \beta = (3\ 4)\,, \quad \gamma = (1\ 3\ 2\ 4)\,.$$

   a) Dire di che tipo di gruppo si tratta.
   b) Dire se esistono in S_4 altri sottogruppi coniugati a G, e quanti sono.

23) Dimostrare che un gruppo di ordine 56 non può essere semplice.

24) Siano A e A' due anelli commutativi ed I, I' due ideali, rispettivamente di A e di A'. Poniamo $J = I \times I'$.
   a) Si mostri che J è un ideale di $A \times A'$.
   b) Si mostri che $(A \times A')/J$ è isomorfo ad $A/I \times A'/I'$.

25) Dimostrare che il polinomio $P(X) = X^4 + X^3 + 1$ è irriducibile in $\mathbb{Z}_2[X]$. Si può dire che è irriducibile anche in $\mathbb{Z}[X]$ o in $\mathbb{Q}[X]$?

26) Siano A e B anelli commutativi con unità e sia $\alpha : A \to B$ un omomorfismo unitario, tale cioè che $\alpha(\mathbf{1}) = \mathbf{1}$.
   a) Si mostri che, se I è un ideale primo di B, allora $\alpha^{-1}(I)$ è un ideale primo di A e che inoltre, se I è un ideale proprio, anche $\alpha^{-1}(I)$ lo è.
   b) Si consideri il caso particolare in cui $A = B = \mathbb{C}[X]$, dove X è una indeterminata, e $\alpha(\sum a_i X^i) = \sum a_i X^{2i}$. Dire, per ogni ideale primo J in A, quali e quanti sono gli ideali primi I di B tali che $\alpha^{-1}(I) = J$.

Prova scritta del 23 settembre 1997

27) Siano G e L due gruppi. Sia H un sottogruppo di G e sia K un sottogruppo di L. Mostrare che $H \times K$ è un sottogruppo normale di $G \times L$ se e solo se H è normale in G e K è normale in L.

28) Per ogni intero positivo pari n indichiamo con D_n il gruppo diedrale di ordine n. Sia G un gruppo di ordine 3. VERO o FALSO: D_{30} è isomorfo al prodotto diretto $D_{10} \times G$.

29) Trovare il numero dei sottogruppi del gruppo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

30) Sia A l'anello $\mathbb{Z}/(5)$ degli interi modulo 5 e si considerino i polinomi $P(X) = X^3 + 2X^2 + 3X + 4$ e $Q(X) = X^3 + X^2 + 3$ in $A[X]$. Siano I e J gli ideali generati da $P(X)$ e $Q(X)$ in $A[X]$.
   a) Mostrare che l'ideale $I + J$ è principale e trovarne esplicitamente un generatore.
   b) Decomporre $P(X)$ e $Q(X)$ in fattori irriducibili in $A[X]$.

31) Sia A un anello commutativo, e siano I e J due ideali di A. Sia IJ l'insieme di tutte le somme finite $a_1b_1 + a_2b_2 + \cdots + a_nb_n$, dove $a_i \in I$ e $b_i \in J$ per ogni i.
   a) Mostrare che IJ è un ideale di A.
   b) Mostrare che $IJ \subset I \cap J$.
   c) Se A è un dominio a ideali principali e $I = (a)$, $J = (b)$, trovare un generatore di IJ.
   d) Mostrare con un esempio che IJ può essere diverso da $I \cap J$.

Prova scritta del 24 ottobre 1997

32) Sia G un gruppo ciclico con 18 elementi. Determinare il gruppo degli automorfismi di G.

33) Dimostrare che ogni 5-sottogruppo di Sylow di S_{10} è isomorfo al prodotto diretto di due gruppi ciclici di ordine 5.

34) Sia A un anello commutativo con $\mathbf{1}$. Sia X l'insieme degli elementi di A che non sono divisori di zero, e sia U l'insieme degli elementi invertibili di A. Mostrare che:
   a) il prodotto di due qualsiasi elementi di X appartiene a X;
   b) $U \subset X$;
   c) se A consta di un numero finito di elementi allora $U = X$.

35) Dire se i seguenti polinomi sono irriducibili o meno in $\mathbb{Q}[X]$:
   a) $X^4 + X^3 + X - 1$;
   b) $X^4 + 3X + 3$;
   c) $X^3 + 6X^2 + 5X + 25$.

36) Sia K un campo, sia $A = K[a_1, \ldots, a_n]$, e sia M un ideale massimale di A.
   a) Si mostri che A/M è un ampliamento algebrico di K.
   b) Se ne deduca che, se $K = \mathbb{C}$, allora l'omomorfismo composto $\mathbb{C} \to A \to A/M$ è un isomorfismo.
   c) Cosa si può dire nel caso in cui $K = \mathbb{R}$?

Prova scritta del 3 febbraio 1998

37) Indichiamo con Q il quadrigruppo. Vero o falso: $Q \times \mathbb{Z}/3\mathbb{Z}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

38) Determinare il gruppo degli automorfismi di S_3.

39) Vero o falso: Se I e J sono ideali primi in un anello commutativo con unità A, allora $I \times J$ è primo in $A \times A$.

40) Sia p un numero primo. Indichiamo con A l'anello quoziente $\mathbb{Z}[X]/(pX)$. Indichiamo con a e b le immagini di p e X in A. Mostrare che gli ideali (a) e(b) sono primi e che l'insieme dei divisori di zero di A è $(a) \cup (b)$.

41) Sia $P(X) \in \mathbb{Z}_3[X]$ il polinomio $X^3 - X + 1$. Si mostri che P è irriducibile in $\mathbb{Z}_3[X]$. Si mostri che, se ζ è una radice di P, anche $\zeta + 1$ e $\zeta - 1$ sono radici. Si calcoli il grado del campo di spezzamento di P su $\mathbb{Z}_3$.

Prova scritta del 2-4-98

Risolvere almeno tre dei seguenti esercizi.

42) Decomporre in prodotto di cicli disgiunti e in prodotto di trasposizioni le seguenti permutazioni

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 2 & 1 & 4 & 6 & 8 & 5 & 3 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 1 & 5 & 6 & 4 & 2 & 7 \end{pmatrix}$$

43) Sia $\mathbb{C}^\times$ il gruppo dei numeri complessi diversi da 0, con l'operazione di moltiplicazione. Sia R l'insieme della radici di 1, cioè l'insieme dei numeri complessi ζ tali che $\zeta^n = 1$ per qualche intero n. Si mostri che R è un sottogruppo di $\mathbb{C}^\times$.

44) Si mostri che ogni gruppo di ordine 153 è abeliano. Si mostri con un esempio che esistono gruppi di ordine 153 non ciclici.

45) Sia G un gruppo finito, sia N un suo sottogruppo normale e sia H un sottogruppo di G contenente N. Mostrare che il numero dei coniugati di H/N in G/N è pari al numero dei coniugati di H in G.

46) Sia G un gruppo finito e sia H un suo sottogruppo di indice 3. Si mostri che il numero dei coniugati distinti di H è 3 (Suggerimento: usare il teorema di Cayley e le sue varianti).

Prova scritta del 28 maggio 1998

Svolgere quattro dei seguenti esercizi.

47) Decomporre in prodotto di cicli disgiunti e di trasposizioni le seguenti permutazioni:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 6 & 7 & 5 & 1 & 4 \end{pmatrix}; \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 2 & 8 & 5 & 6 \end{pmatrix}.$$

48) Indichiamo con C_n il gruppo ciclico di ordine n, e poniamo $G = C_3 \times C_7$. Si mostri che il gruppo degli automorfismi di G è un gruppo abeliano non ciclico di ordine 12.

49) Si mostri che ogni gruppo di ordine 1225 è abeliano.

50) Sia A un anello commutativo con unità e sia I un suo ideale. Si mostri che ogni elemento di $A - I$ è invertibile se e solo se ogni ideale proprio di A è contenuto in I. In questo caso si mostri anche che, se A è un dominio euclideo, allora vi è un elemento $t \in I$ con la proprietà che ogni ideale di A è generato da una potenza di t.

51) Sia K il campo con 11 elementi, e sia $P(X) = X^3 - 2 \in K[X]$. Indichiamo con I l'ideale in $K[X]$ generato da P, e poniamo $F = K[X]/I$. Si mostri che F non è un campo e si calcoli il numero dei suoi elementi.

Prova scritta del 25 giugno 1998

Risolvere quattro dei seguenti esercizi

52) Dire quali tra le seguenti permutazioni sono pari e quali dispari:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 1 & 4 & 2 & 3 & 8 & 9 & 7 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 5 & 3 & 8 & 4 & 1 & 2 \end{pmatrix},$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 7 & 1 & 4 & 6 & 9 & 3 & 8 \end{pmatrix}.$$

53) Sia G il gruppo diedrale di ordine 12. Trovare il centro di $G \times S_3$.

54) Si mostri che ogni gruppo di ordine 56 ha un sottogruppo di Sylow normale.

55) Poniamo $A = \mathbb{Z}[\sqrt{2}]$.
   a) Si mostri che ogni elemento di A si scrive, in modo unico, sotto la forma $a + b\sqrt{2}$, dove a e b sono interi.
   b) Si mostri che l'applicazione $\varphi : A \to A$ data da $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ è un automorfismo.

   Per ogni $z \in A$ poniamo $N(z) = z\varphi(z)$
   c) Si mostri che $N(z)$ è un intero e che $N(zw) = N(z)N(w)$.
   d) Si mostri che z è invertibile in A se e solo se $N(z) = \pm 1$.

56) Sia I l'ideale in $\mathbb{Z}[X]$ che è generato da 5 e da $P = X^3 - 3X^2 + 1$. Si mostri che I è massimale.

Prova scritta del 15 settembre 1998

Risolvere quattro dei seguenti esercizi.

57) Trovare tutti gli ordini possibili di elementi di S_7.

58) Descrivere, a meno di isomorfismo, tutti i gruppi di ordine 55.

59) **Vero o Falso:** esistono gruppi finiti non abeliani G tali che $G/Z(G)$ sia abeliano, dove $Z(G)$ denota il centro di G.

60) Sia (A, d) un dominio euclideo con unità, e si supponga che la sua funzione "grado" d abbia la proprietà che, se $a + b \neq 0$ allora $d(a + b) \geq \min(d(a), d(b))$. Si mostri che:
   a) $M = \{a \in A : d(a) > d(1)\} \cup \{0\}$ è un ideale in A.
   b) Ogni elemento di $A - M$ è invertibile.

61) Sia $\mathbb{F}_5$ il campo con 5 elementi, e sia K il campo di spezzamento su $\mathbb{F}_5$ del polinomio $P(X) = X^3 - X^2 - 4$. Si calcolino $[K : \mathbb{F}_5]$ e il numero di elementi di K. Si mostri che $X^2 - 2$ ha una radice in K.

Prova scritta del 27 ottobre 1998

Risolvere quattro dei seguenti esercizi.

62) Trovare tutti gli elementi di S_5 che commutano con

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

63) Sia G il gruppo diedrale di ordine $2k$. Trovare tutti i sottogruppi normali di G.

64) Si mostri che un gruppo di ordine 80 non può essere semplice.

65) Trovare tutti gli ideali propri di $\mathbb{Z}_{45}$. Dire quali tra essi sono primi e quali massimali.

66) Se p è un numero primo, indichiamo con $\mathbb{F}_{p^h}$ il campo con p^h elementi.
   a) Mostrare che, se $h \leq 3$, la sola radice quinta di 1 in $\mathbb{F}_{3^h}$ è 1.
   b) Sia K il campo di spezzamento di $X^5 - 1$ su $\mathbb{F}_3$. Mostrare che $[K : \mathbb{F}_3] = 4$.

Prova scritta del 5 febbraio 1999

67) Sia G il sottoinsieme di S_5 costituito da tutte le permutazioni σ tali che $\sigma(\{1, 2\}) = \{1, 2\}$. Si mostri che G è un sottogruppo di S_5 e se ne calcoli l'ordine.

68) Sia G un gruppo di ordine 27, e sia H un suo sottogruppo di ordine 9. Si mostri che H contiene elementi del centro di G diversi da 1.

69) Sia K un campo, e sia X una indeterminata su K. Si mostri che tutti gli elementi di $K[X]$ che non appartengono a K sono trascendenti su K.

70) Sia A l'anello $\mathbb{R}[a_1, \ldots, a_n]$, dove $a_1, \ldots, a_n$ sono elementi di un sovranello commutativo di $\mathbb{R}$; sia M un ideale massimale di A.
   a) Si mostri che A/M è isomorfo a $\mathbb{R}$ o a $\mathbb{C}$.
   b) Si dia un esempio per ognuno dei due casi descritti al punto a).

Soluzioni

1) Sia x un elemento di $(A \odot B) \odot C$. Dunque x appartiene ad $A \odot B$ o a C ma non a tutti e due. Analogamente, dire che x appartiene ad $A \odot B$ significa che x appartiene ad A o a B ma non a tutti e due. Le possibilità sono:

- $x \in C$ e $x \notin A \odot B$, cioè
  - $x \in C$ e $x \notin A$, $x \notin B$
    oppure
  - $x \in C$ e $x \in A \cap B$, cioè $x \in A \cap B \cap C$

  oppure
- $x \notin C$ e $x \in A \odot B$, cioè
  - $x \notin C$ e $x \in A$, $x \notin B$
    oppure
  - $x \notin C$ e $x \notin A$, $x \in B$

In altri termini, le possibilità sono:

- $x \in A$, $x \notin B$, $x \notin C$
  oppure
- $x \notin A$, $x \in B$, $x \notin C$
  oppure
- $x \notin A$, $x \notin B$, $x \in C$
  oppure
- $x \in A$, $x \in B$, $x \in C$

Dunque

$$(A \odot B) \odot C = (A \cup B \cup C - ((A \cap B) \cup (A \cap C) \cup (B \cap C))) \cup (A \cap B \cap C)\,.$$

Lo stesso ragionamento mostra che il lato destro di questa uguaglianza è uguale anche ad $A \odot (B \odot C)$.
È chiaro che $A \odot B = B \odot A$. Sia ora A un sottinsieme di X. Si ha che

$$A \odot \emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A - \emptyset = A\,.$$

Ciò significa che $\emptyset$ è un elemento neutro per l'operazione $\odot$. Poi

$$A \odot A = (A \cup A) - (A \cap A) = A - A = \emptyset\,,$$

cioè ogni elemento di $\mathcal{P}(X)$ è inverso di sè stesso.

2) VERO. Sia h un elemento di H; vi è un intero positivo n tale che $h^n = \mathbf{1}$. Se g è un elemento di G, allora

$$(ghg^{-1})^n = \underbrace{ghg^{-1}ghg^{-1}\dots ghg^{-1}}_{n \text{ volte}} = g\underbrace{h\dots h}_{n \text{ volte}}g^{-1} = gh^ng^{-1} = gg^{-1} = \mathbf{1}\,,$$

e quindi $ghg^{-1} \in H$. Ciò significa che, per ogni $g \in G$, $gHg^{-1} \subset H$. Si ha dunque anche $g^{-1}Hg = g^{-1}H(g^{-1})^{-1} \subset H$. Moltiplicando a sinistra per g e a destra per g^{-1}

se ne deduce che $H \subset gHg^{-1}$. In conclusione $gHg^{-1} = H$ per ogni $g \in G$, cioè H è normale.

3) Siano n e m gli ordini di H e K. Dunque l'ordine di $H \times K$ è nm. D'altra parte, se $(a, b)^l = \mathbf{1}_{H\times K}$, allora $a^l = \mathbf{1}_H$ e $b^l = \mathbf{1}_K$, e quindi l è multiplo sia di n che di m. Visto che n e m sono primi fra loro, l è divisibile per nm. Ne segue che l'ordine di (a, b) è nm. Il sottogruppo (ciclico) di $H \times K$ generato da (a, b) ha dunque nm elementi, come $H \times K$, e quindi è uguale ad $H \times K$.

4) Pari. Infatti α si può scrivere come prodotto di cicli o di trasposizioni come segue:

$$\alpha = (1\ 2\ 5)(3\ 8)(4\ 7\ 6\ 9) = (1\ 2)(1\ 5)(3\ 8)(4\ 7)(4\ 6)(4\ 9)$$

5)

$$\begin{aligned}
\alpha \circ \beta(x) &= (3x + 2)^2 + 1 = 9x^2 + 12x + 5 \\
\beta \circ \alpha(x) &= 3(x^2 + 1) + 2 = 3x^2 + 5 \\
\alpha^2(x) &= (x^2 + 1)^2 + 1 = x^4 + 2x^2 + 2 \\
\beta^2(x) &= 3(3x + 2) + 2 = 9x + 8
\end{aligned}$$

6) Basta contare le applicazioni iniettive da $\{1, 2, 3, 4, 5\}$ in $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Indichiamo con α una tale applicazione. Vi sono 8 possibilità per $\alpha(1)$. Una volta fissato $\alpha(1)$, i valori possibili per $\alpha(2)$ sono 7, in quanto il valore $\alpha(1)$ è vietato per l'iniettività di α. Analogamente, una volta fissati $\alpha(1)$ e $\alpha(2)$, i valori possibli per $\alpha(3)$ sono solo 6, e cosí via. In totale, le possibilità per α sono

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = \frac{8!}{(8 - 5)!} = 6720\,.$$

In generale, le applicazioni iniettive da X a Y sono

$$k \cdot (k - 1) \cdots (k - h + 1) = \frac{k!}{(k - h)!}\,.$$

7) La composizione di applicazioni è associativa. Inoltre l'applicazione identità $\mathbf{1}_X$ è un elemento neutro in quanto $\mathbf{1}_X \circ f = f = f \circ \mathbf{1}_X$ per ogni applicazione f di X in sè. Il problema è dunque stabilire quando ogni applicazione di X in sè abbia un inversa, cioè sia biunivoca. Questo è senz'altro vero quando X consta di un solo elemento, ed è falso in tutti gli altri casi. Infatti, se X contiene piú di un elemento e a è uno di questi, l'applicazione f definita da $f(x) = a$ per ogni $x \in X$ non è iniettiva, e quindi in particolare non è biunivoca.

8) Sia $G = S_3$, e siano x e y le permutazioni

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

L'ordine di x è 2 e quello di y è 3, mentre l'ordine di

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

è 2. Supponiamo ora che G sia abeliano. Scriviamo $h = h'm$, e $k = k'm$; è chiaro che h' e k' sono interi primi fra loro. Sia ora n un intero divisibile per h e per k. Dato che G è abeliano possiamo scrivere

$$(xy)^n = \underbrace{xy \dots xy}_{n \text{ volte}} = x^m y^n = \mathbf{1}\,.$$

Dato che $hk/m = h'k'm$ è divisibile sia per h che per k, ne segue che l'ordine di xy è un suo divisore. Supponiamo viceversa che $(xy)^l = \mathbf{1}$. Allora, dato che G è abeliano,

$$\mathbf{1} = (xy)^{lh} = (x^h)^l y^{lh} = y^{lh}\,,$$

e dunque $lh = lmh'$ è divisibile per l'ordine di y, cioè per $k = mk'$. Ne segue che $k' \big| lh'$ e quindi, dato che h' e k' sono primi fra loro, che $k' \big| l$. Analogamente si conclude che $h' \big| l$, e quindi, sempre perchè h' e k' sono primi fra loro, che l è divisibile per $h'k' = hk/m^2$.

9) Induzione su n. Se $n = 1$, X ha due soli sottinsiemi, cioè X e $\emptyset$; tra questi, solo il secondo ha un numero pari di elementi. Dunque X ha $1 = 2^{1-1}$ sottinsiemi con un numero pari di elementi. Supponiamo ora, induttivamente, di sapere che quanto affermato è vero per gli insiemi con meno di n elementi. Notiamo che, poiché un insieme con k elementi ha 2^k sottinsiemi, segue dall'ipotesi induttiva che, se Y è un insieme con $k < n$ elementi, anche i sottinsiemi di Y con un numero dispari di elementi sono 2^{k-1}. Fissiamo un elemento x di X, e poniamo $Y = X - \{x\}$. I sottinsiemi di X con un numero pari di elementi sono di due tipi: quelli che non contengono x e quelli che lo contengono. I primi sono i sottinsiemi di Y con un numero pari di elementi, e per ipotesi induttiva ve ne sono 2^{n-2}. I secondi sono della forma $A \cup \{x\}$, dove A è un sottinsieme di Y con un numero dispari di elementi. Anche di questi, per quanto osservato sopra, ce ne sono 2^{n-2}. In totale dunque i sottinsiemi di X con un numero pari di elementi sono $2^{n-2} + 2^{n-2} = 2^{n-1}$.
(Ragionamento alternativo per n dispari. Se A è un sottinsieme di X, poniamo $\alpha(A) = X - A$. Se $\mathcal{P}(X)$ è l'insieme di tutti i sottinsiemi di X, α è una applicazione di $\mathcal{P}(X)$ in sè, che è biunivoca in quanto α^2 è l'identità su $\mathcal{P}(X)$. Inoltre, se A contiene un numero pari di elementi, $\alpha(A)$ ne contiene un numero dispari, e viceversa. Dunque α stabilisce una corrispondenza biunivoca tra sottinsiemi di X con un numero pari di elementi e sottinsiemi con un numero dispari di elementi; vi sono dunque tanti sottinsiemi del primo tipo quanti del secondo tipo. Dato che i sottinsiemi di X sono complessivamente 2^n, quelli con un numero pari di elementi sono 2^{n-1}.)

10) Siano g e g' elementi di H. Allora $\varphi(gg') = \varphi(g)\varphi(g') = gg'$, dunque $gg' \in H$. Poiché G è finito questo mostra che H è un sottogruppo (anche se G non è abeliano). Se

invece g e g' appartengono a K, $\varphi(gg') = \varphi(g)\varphi(g') = g^{-1}g'^{-1} = (g'g)^{-1} = (gg')^{-1}$ perhè G è abeliano, dunque $gg' \in K$. Quindi anche K è un sottogruppo. Se $g \in H \cap K$, allora $g = \varphi(g) = g^{-1}$, cioè $g^2 = \mathbf{1}$. I casi possibili sono quindi a priori due: o $g = \mathbf{1}$ oppure g ha ordine 2; in questo secondo caso però, per il teorema di Lagrange, G dovrebbe avere ordine pari, contro le ipotesi.

11) Se $g, g' \in G_n$ e G è abeliano, allora

$$(g^{-1}g')^n = g^{-n}g'^n = (g^n)^{-1}g'^n = \mathbf{1} \cdot \mathbf{1} = \mathbf{1}\,,$$

e quindi $g^{-1}g' \in G_n$. Invece, se $n = 2$ e $G = S_3$, allora G_n non è un sottogruppo di G. Infatti le permutazioni

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

hanno ordine 2 ma il loro prodotto

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

ha ordine 3 e quindi non appartiene a G_n.
Supponiamo infine di sapere che G_n è un sottogruppo di G, e sia h un elemento di G_n. Per ogni $g \in G$ si ha che

$$(ghg^{-1})^n = \underbrace{ghg^{-1}ghg^{-1}\dots ghg^{-1}}_{n \text{ volte}} = gh^ng^{-1} = g\mathbf{1}g^{-1} = \mathbf{1}\,,$$

e dunque anche ghg^{-1} appartiene a G_n. Questo mostra che $gG_ng^{-1} \subset G_n$ per ogni $g \in G$. Dunque è anche vero che $g^{-1}G_ng = g^{-1}G_n(g^{-1})^{-1} \subset G_n$ per ogni $g \in G$. Moltiplicando a sinistra per g e a destra per g^{-1} si conclude che $G_n \subset gG_ng^{-1}$, e quindi che $gG_ng^{-1} = G_n$ per ogni $g \in G$. Ciò significa che G_n è un sottogruppo normale.

12) I sottogruppi di un gruppo ciclico infinito sono tutti ciclici infiniti, dunque G deve essere un gruppo finito. Sia n il suo ordine, e sia g un suo generatore. Per il teorema di Lagrange, n deve essere divisibile sia per 20 che per 84. Quindi n deve essere divisibile per il minimo comune multiplo di 20 e 84, cioè per 420. Si sa che un generatore di H è g^a, dove $a = n/20$, e che uno di K è g^b, dove $b = n/84$. Ancora per il teorema di Lagrange, l'ordine di $H \cap K$ deve dividere il massimo comun divisore di 20 e 84, cioè 4. D'altra parte $n/4$ è multiplo sia di a che di b, quindi $g^{n/4}$, che ha ordine 4, appartiene sia ad H che a K. In conclusione $o(H \cap K) = 4$.

13) Sia S un sistema finito di generatori per G, e poniamo $T = \alpha(S)$. Dico che T genera K. Infatti, se $k \in K$, possiamo scrivere $k = \alpha(g)$ per qualche $g \in G$, e $g = s_1s_2 \cdots s_n$, dove gli s_i sono elementi di S. Dunque $k = \alpha(g) = \alpha(s_1s_2 \cdots s_n) = \alpha(s_1) \cdots \alpha(s_n)$ è prodotto di elementi di T.

14) In un gruppo abeliano due sottogruppi sono coniugati se e solo se coincidono. Basta dunque trovare un gruppo abeliano finito G con due sottogruppi distinti di ordine p^n. Per esempio si può porre $G = H \times H$, dove H è ciclico di ordine p^n; i sottogruppi $H_1 = H \times \{\mathbf{1}\}$ e $H_2 = \{\mathbf{1}\} \times H$ hanno ordine p^n e sono distinti.

15) I 17-sottogruppi di Sylow sono $n = 1 + k \cdot 17$, dove $n \big| 5 \cdot 13 = 65$. Dato che 64 non è divisibile per 17, deve essere $n = 1$. Quindi G ha un solo 17-sottogruppo di Sylow H, che è normale. Il quoziente G/H ha ordine $5 \cdot 13$. Dato che $5 \not| 12 = 13 - 1$, G/H è abeliano. Esattamente allo stesso modo si dimostra che G contiene un unico 13-sottogruppo di Sylow K, che questo è normale, e che il quoziente G/K è abeliano. Ne segue che il gruppo dei commutatori di G è contenuto sia in H che in K, e dunque in $H \cap K$. D'altra parte $H \cap K$ è un sottogruppo sia di H che di K, quindi il suo ordine divide sia 13 che 17, e perciò vale 1. Si conclude che G è abeliano perchè il suo gruppo dei commutatori è $\{\mathbf{1}\}$.

16) Supponiamo H normale, e sia $\beta : K \to K/H$ l'omorfismo naturale. Allora $H = \beta^{-1}(\{\mathbf{1}_{K/H}\})$, e dunque $\alpha^{-1}(H) = (\beta \circ \alpha)^{-1}(\{\mathbf{1}_{K/H}\})$; in altre parole $\alpha^{-1}(H)$ è il nucleo di $\beta \circ \alpha$ e quindi è normale. Supponiamo viceversa che $\alpha^{-1}(H)$ sia normale, e sia $\gamma : G \to G/\alpha^{-1}(H)$ la proiezione naturale. Dato che $\alpha^{-1}(H) \supset \ker(\alpha)$, vi è un (unico) omomorfismo $\eta : K \to G/\alpha^{-1}(H)$ tale che $\gamma = \eta \circ \alpha$. Il nucleo di η è $\alpha(\alpha^{-1}(H) = H$. Quindi H è normale.

17) Sia G un gruppo di ordine $99 = 11 \cdot 3^2$. Siano a e b i numeri dei 3-sottogruppi di Sylow e degli 11-sottogruppi di Sylow. Dato che $a = 1 + k \cdot 3$ e che a divide 11, necessariamente $a = 1$. Analogamente b è della forma $1 + h \cdot 11$ e divide 9, quindi è uguale a 1. Dunque vi sono un unico 3-sottogruppo di Sylow H e un unico 11-sottogruppo di Sylow K. In particolare H e K sono normali e quindi $G = H \times K$. Inoltre H è abeliano perchè il suo ordine è il quadrato di un primo e K è ciclico perchè ha ordine primo. Dunque G è abeliano.

18) Sia G un gruppo infinito. Se G contiene un elemento g di ordine infinito, il sottogruppo generato da g è ciclico infinito e dunque isomorfo a $\mathbb{Z}$, che contiene infiniti sottogruppi. Supponiamo che ogni elemento di G abbia ordine finito. Sia g_1 un elemento di G, e sia G_1 il sottogruppo che esso genera; è un gruppo finito. Scegliamo un elemento g_2 di $G - G_1$ e sia G_2 il sottogruppo che esso genera. Scegliamo poi un elemento g_3 di $G - (G_1 \cup G_2)$ e sia G_3 il sottogruppo che esso genera, e cosí via. I sottogruppi G_1, G_2, ... sono distinti. Quindi G ha infiniti sottogruppi.

19) $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$. Notiamo che $q(X) = X^2 + 1$ è irriducibile perchè non ha radici in K, e poniamo $r(X) = X + 1$. Siano a e b elementi di $K[X]$ e siano $\overline{a}$ e $\overline{b}$ le loro immagini in A. Dire che $\overline{a}\overline{b} = 0$ è lo stesso che dire che $ab \in I$, cioè che $p = qr$ divide ab. Dato che q ed r sono irriducibili, questo significa che o qr divide a, cioè $\overline{a} = 0$, o divide b, cioè $\overline{b} = 0$, oppure q divide uno tra a e b, e r divide l'altro. In definitiva i divisori di zero in A sono le classi dei polinomi divisibili per q o per r ma non per p, cioè dei polinomi che non sono primi con p e non sono divisibili per p. In particolare A contiene divisori di zero e quindi non può essere un campo. Se f è un polinomio primo con p, vi sono polinomi s e t tali che $sf + tp = 1$. Dunque la classe di

f in A è invertibile e il suo inverso è la classe di s. In definitiva gli elementi invertibili di A sono le classi dei polinomi primi con p. Infine

$$X \cdot (-X^2 - X - 1) \equiv 1 \qquad (\text{mod. } p)\,,$$

quindi l'inverso della classe di X è la classe di $-X^2 - X - 1$.

20) Le decomposizioni di $f(X)$ e $g(X)$ in fattori irriducibili sono

$$f(X) = X(X-1)(X^2+2)\,,$$
$$g(X) = (X-1)(2X^2+3)\,.$$

L'ideale I è generato dal massimo comun divisore di $f(X)$ e $g(X)$, cioè da $X-1$. È primo perchè è generato da un polinomio irriducibile ed è massimale perchè, in un dominio a ideali principali come $\mathbb{Q}[X]$, gli ideali primi diversi da $\{0\}$ sono massimali.

21) Siano $x = a/p^n$ e $y = b/p^m$ elementi di R. Moltiplicando numeratori e denominatori per opportune potenze di p possiamo supporre che $n = m$. Dato che

$$x - y = \frac{a-b}{p^n}\,, \qquad xy = \frac{ab}{p^{2n}}\,,$$

$x - y$ e xy appartengono a R. Dunque R è un sottoanello di $\mathbb{Q}$. Sia I un ideale di R, e poniamo $J = I \cap \mathbb{Z}$. Dato che $\mathbb{Z}$ è a ideali principali, $J = h\mathbb{Z}$ per qualche intero h. Dico che $I = hR$. Intanto $hR \subset I$, dato che $h \in I$. Se $x = a/p^n \in I$, allora $a = p^n x \in J$ e dunque $a = kh$ per qualche intero k. Ne segue che $x = (k/p^n) \cdot h \in hR$. Gli ideali di R sono dunque tutti principali, anzi sono della forma hR, dove h è un intero. Resta da decidere quando l'ideale hR è massimale. Notiamo che gli elementi invertibili in R sono le potenze di p e i loro opposti. Ci si può quindi limitare al caso in cui h è primo con p. Osserviamo che in questo caso $hR \cap \mathbb{Z}$ è generato da h. Sia infatti z un elemento di $hR \cap \mathbb{Z}$. Dunque z è della forma $(a/p^n) \cdot h$. Dato che h e p sono primi fra loro, e z è un intero, p^n deve dividere a, e quindi $z \in h\mathbb{Z}$. Da quanto si è detto segue che, se h e k sono interi primi con p, allora $hR \subset kR$ se e solo se $h\mathbb{Z} \subset k\mathbb{Z}$; in particolare hR è massimale in R se e solo se $h\mathbb{Z}$ lo è in $\mathbb{Z}$. Quindi gli ideali massimali in R sono quelli della forma qR, dove q è un numero intero primo e diverso da $\pm p$.

22) Sappiamo che α ha ordine 2 e γ ha ordine 4. Inoltre si calcola immediatamente che

$$\gamma\alpha = \alpha\gamma^3$$

Da questa identità segue che il sottogruppo generato da α e da γ consta degli 8 elementi $\mathbf{1}$, γ, γ^2, γ^3, α, $\alpha\gamma$, $\alpha\gamma^2$, $\alpha\gamma^3$ e che si tratta di un gruppo diedrale. Inoltre

$$\alpha\gamma^2 = (3\ 4) = \beta\,,$$

e dunque questo gruppo coincide con G. Osserviamo che G non contiene altre trasposizioni oltre a (1 2) e (3 4). I sottogruppi di S_4 coniugati a G sono quelli generati da

$(\sigma(1)\ \sigma(2))$, $(\sigma(3)\ \sigma(4))$ e $(\sigma(1)\ \sigma(3)\ \sigma(2)\ \sigma(4))$, dove σ è una qualsiasi permutazione in S_4. Sembra dunque che abbiamo a che fare con 24 sottogruppi, includendo G. Vi sono però delle coincidenze. Infatti, se $\sigma = (1\ 2)$, allora $\sigma\alpha\sigma^{-1} = \alpha$, $\sigma\beta\sigma^{-1} = \beta$, mentre $\sigma\gamma\sigma^{-1} = \gamma^{-1}$, e quindi $\sigma G\sigma^{-1} = G$. Lo stesso accade se $\sigma = (3\ 4)$. Se invece $\sigma = (1\ 3)(2\ 4)$, allora $\sigma\alpha\sigma^{-1} = \beta$, $\sigma\beta\sigma^{-1} = \alpha$, mentre $\sigma\gamma\sigma^{-1} = \gamma^{-1}$, e quindi anche in questo caso $\sigma G\sigma^{-1} = G$. Ma il sottogruppo di S_4 generato da $(1\ 2)$, $(3\ 4)$ e $(1\ 3)(2\ 4)$ consta di 8 elementi, quindi G ha al piú $24/8 = 3$ coniugati, incluso G stesso. Tra questi ci sono quello generato da $(1\ 3)$, $(2\ 4)$ e $(1\ 2\ 3\ 4)$ e quello generato da $(1\ 4)$, $(2\ 3)$ e $(1\ 2\ 4\ 3)$, che sono distinti e diversi da G perchè contengono trasposizioni diverse. Dunque G ha esattamente tre coniugati.

23) $56 = 7 \cdot 2^3$. Il numero dei 7-sottogruppi di Sylow di un gruppo G di ordine 56 è della forma $1 + 7k$ e divide 8, dunque può essere 1 o 8. Se G ha un solo 7-sottogruppo di Sylow, questo è normale, e G non è semplice. Se invece G ha 8 7-sottogruppi di Sylow, il sottinsieme di G costituito dagli elementi di ordine 7, che indichiamo con S, consta di $8(7-1) = 48$ elementi. Se H è un 2-sottogruppo di Sylow di G, H ha 8 elementi e non contiene elementi di ordine 7, cioè $H \cap S = \emptyset$. Dunque $H = G - S$. Questo mostra che G ha un solo 2-sottogruppo di Sylow, che è necessariamente normale, e quindi G non è semplice.

24) Siano $\alpha : A \to A/I$ e $\alpha' : A' \to A'/I'$ gli omomorfismi di passaggio al quoziente, e definiamo una applicazione $\beta : A \times A' \to A/I \times A'/I'$ ponendo $\beta(a, a') = (\alpha(a), \alpha'(a'))$. Questa applicazione è un omomorfismo suriettivo di anelli. Il suo nucleo è

$$\{(a, a') : \alpha(a) = 0, \alpha'(a') = 0\} = I \times I' = J\,.$$

Ne segue che $J = I \times I'$ è un ideale e, per il teorema di omorfismo, che $A/I \times A'/I'$ è isomorfo ad $(A \times A')/J$.

25) P non ha radici in $\mathbb{Z}_2$ perchè $P(0) = 1 = P(1)$; ne segue che P non ha fattori di grado 1. Se P non è irriducibile è divisibile per un polinomio monico di grado 2. Ora i polinomi di grado 2 in $\mathbb{Z}_2[X]$ sono X^2, $X^2 + 1 = (X + 1)^2$ e $Q(X) = X^2 + X + 1$. Visto che P non è divisibile per polinomi di grado 1, per dimostrare che è irriducibile basta mostrare che non è divisibile per Q. Se lo fosse, detta a una radice di Q in un ampliamento di $\mathbb{Z}_2$, si dovrebbe avere che $P(a) = 0$. Ma dire che $Q(a) = 0$ significa dire che $a^2 = a+1$, e quindi $P(a) = (a^2)^2 + aa^2 + 1 = (a+1)^2 + a(a+1) + 1 = a+1+1 = a$. Dato che $Q(0) \neq 0$, $a \neq 0$, e quindi a non è radice di P.
P è irriducibile anche in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$. Infatti, se non fosse irriducibile in $\mathbb{Z}[X]$, potremmo scrivere $P = RS$, dove R e S sono polinomi a coefficienti interi monici e di grado positivo. Riducendo questa fattorizzazione modulo 2 si ottiene una fattorizzazione di P come prodotto di polinomi di grado positivo in $\mathbb{Z}_2[X]$, contro l'irriducibilità di P in $\mathbb{Z}_2[X]$. Il lemma di Gauss dice poi che, dato che P è irriducibile in $\mathbb{Z}[X]$, lo è anche in $\mathbb{Q}[X]$.

26) a) Se $a, b \in A$ e $ab \in \alpha^{-1}(I)$, cioè se $\alpha(a)\alpha(b) = \alpha(ab) \in I$, allora o $\alpha(a) \in I$ oppure $\alpha(b) \in I$, dato che I è primo. In altri termini o $a \in \alpha^{-1}(I)$ oppure $b \in \alpha^{-1}(I)$.

Questo mostra che $\alpha^{-1}(I)$ è primo. Se poi $I \neq B$ allora $\alpha(\mathbf{1}) = \mathbf{1} \notin I$, quindi $\mathbf{1} \notin \alpha^{-1}(I)$, e dunque $\alpha^{-1}(I) \neq A$.

b) Ogni ideale di $A = B = \mathbb{C}[X]$ è principale; gli ideali primi diversi da A e $\{0\}$ sono quelli generati da polinomi irriducibili, che possiamo supporre monici; per il "teorema fondamentale dell'algebra" questi sono esattamente i polinomi di primo grado. Siano $P(X) = X - a$ e $Q(X) = X - b$ due di essi. Dire che $\alpha^{-1}((Q)) = (P)$ equivale a dire che $\alpha(P) \in (Q)$. È infatti chiaro che questa è una condizione necessaria. Per vederne la sufficienza notiamo che, se vale, allora $(P) \subset \alpha^{-1}((Q))$. Ma dato che in un anello a ideali principali ogni ideale primo non banale è massimale, e $\alpha^{-1}((Q))$ è un ideale proprio, deve essere $(P) = \alpha^{-1}((Q))$. Ora $\alpha(P) = X^2 - a$, e dire che appartiene all'ideale generato da Q significa che Q ne è un fattore. Dato che la fattorizzazione di $X^2 - a$ è $(X - c)(X + c)$ dove $c^2 = a$, deve allora essere $b = c$ o $b = -c$. In definitiva gli ideali primi la cui immagine inversa è J sono quelli generati da $X - c$ e da $X + c$. Questi polinomi non sono associati, e quindi gli ideali che essi generano sono distinti, a meno che non si abbia $c = 0$, cioè $a = 0$. Gli ideali cercati sono quindi in numero di uno o due, a seconda che sia $a = 0$ o $a \neq 0$. Il solo ideale primo la cui immagine inversa sia A è B e il solo la cui immagine inversa sia $\{0\}$ è $\{0\}$ (notare che α è iniettiva).

27) Supponiamo che H e K siano normali in G e L. Siano $\alpha : G \to G/H$ e $\beta : L \to L/K$ gli omomorfismi "passaggio al quoziente" e definiamo una applicazione $\gamma : G \times L \to G/H \times L/K$ ponendo $\gamma(g, l) = (\alpha(g), \beta(l))$. Si verifica subito che γ è un omomorfismo. Inoltre $\gamma(g, l) = \mathbf{1}$ se e solo se $\alpha(g) = \mathbf{1}$, $\beta(l) = \mathbf{1}$. In altre parole, il nucleo di γ è $H \times K$, che quindi è normale.
Supponiamo invece che $H \times K$ sia normale. Sia $\xi : G \times L \to (G \times L)/(H \times K)$ l'omomorfismo "passaggio al quoziente", sia $\vartheta : G \to G \times L$ l'omomorfismo $\vartheta(g) = (g, \mathbf{1})$, e sia $\eta = \xi \circ \vartheta$ la loro composizione. Dire che $\eta(g) = \mathbf{1}$ equivale a dire che $\xi(g, \mathbf{1}) = \mathbf{1}$, cioè che $(g, \mathbf{1}) \in H \times \{\mathbf{1}\}$ o, ancora, che $g \in H$. In altre parole, il nucleo di η è H, che quindi è normale. Lo stesso ragionamento mostra che anche K è normale.

28) Falso. Ricordiamo che un gruppo diedrale di ordine $2n$ è generato da un elemento a di ordine n e da uno b di ordine 2, soggetti alla relazione $ab = ba^{-1}$. Ne segue che $(a^h b)^2 = ba^{-h}a^h b - = b^2 = \mathbf{1}$ per ogni h. Se n è dispari questo implica che in D_{2n} ci sono esattamente n elementi di ordine 2. In particolare D_{30} e D_{10} contengono, rispettivamente, 15 e 5 elementi di ordine 2. Se (h, g) è un elemento di ordine 2 di $D_{10} \times G$, allora $h^2 = \mathbf{1}$ e $g^2 = \mathbf{1}$. Dato che G non contiene elementi di ordine 2 ne segue che h ha ordine 2 e $g = \mathbf{1}$. Dunque gli elementi di ordine 2 di $D_{10} \times G$ sono 5, e non 15.

29) Poniamo $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$. Gli elementi non nulli di G sono a, b, c, $a + b$, $a + c$, $b + c$ e $a + b + c$, che hanno tutti ordine 2. L'ordine di un sottogruppo di G deve dividere l'ordine di G, che è 8. I sottogruppi diversi dai sottogruppi banali $\{0\}$ e G possono dunque avere ordine 2 o 4. I sottogruppi di ordine 2 sono quelli generati dagli elementi di G di ordine 2; ve n'è quindi uno per ogni elemento non nullo di G. Dato che, dividendo G per un suo sottogruppo di ordine 4, si ottiene un gruppo che è canonicamente isomorfo a $\mathbb{Z}/2\mathbb{Z}$, i sottogruppi di ordine 4 sono i nuclei degli

omomorfismi suriettivi di G su $\mathbb{Z}/2\mathbb{Z}$. Ognuno di questi omomorfismi è univocamente determinato dalle immagini di a, b e c. Le possibilità sono

immagine di a	immagine di b	immagine di c
1	0	0
0	1	0
0	0	1
1	1	0
1	0	1
0	1	1
1	1	1

Vi sono dunque 7 sottogruppi di ordine 4. Dunque G ha in tutto 16 sottogruppi.

30) $A[X]$ è a ideali principali perchè è un anello di polinomi su un campo; quindi ogni suo ideale, e in particolare $I+J$, è principale. Un generatore di $I+J$ è il massimo comun divisore di P e Q. Per trovarlo usiamo l'algoritmo euclideo:

$$\begin{aligned} P(X) &= Q(X) + X^2 + 3X + 1 \\ P(X) &= (X-1)(X^2+3X+1) + 5X + 5 \equiv (X-1)(X^2+3X+1) \mod 5\,. \end{aligned}$$

Dunque il massimo comun divisore di P e Q modulo 5 è X^2+3X+1. Inoltre

$$Q(X) = (X-2)(X^2+3X+1) + 5X + 5 \equiv (X-2)(X^2+3X+1) \mod 5\,.$$

D'altra parte 1 è chiaramente una radice di X^2+3X+1 modulo 5, e un'altra divisione dà

$$X^2 + 3X + 1 = (X-1)(X+4) + 5 \equiv (X-1)^2 \mod 5\,.$$

in conclusione le decomposizioni di P e Q in fattori irriducibili sono

$$\begin{aligned} P(X) &\equiv (X-1)^3 \mod 5\,, \\ Q(X) &\equiv (X-2)(X-1)^2 \mod 5\,. \end{aligned}$$

31) È chiaro che la somma di due elementi di IJ appartiene ancora a IJ. Se $x = \sum a_i b_i \in IJ$, dove $a_i \in I$ e $b_i \in J$, e $c \in A$, allora $cx = \sum (ca_i) b_i$ appartiene a IJ perchè $ca_i \in I$ per ogni i, dato che I è un ideale. Se $a \in I$ e $b \in J$, allora $ab \in I$ e $ab \in J$ perchè I e J sono ideali; lo stesso si può dire per le somme $\sum a_i b_i$, dove $a_i \in I$ e $b_i \in J$. Dunque $IJ \subset I \cap J$. Supponiamo ora che A sia a ideali principali e che $I = (a)$, $J = (b)$. Dico che $IJ = (ab)$. Infatti, da una parte $ab \in IJ$, e quindi $(ab) \subset IJ$. Se invece $x = \sum a_i b_i \in IJ$, dove $a_i \in I$ e $b_i \in J$, allora possiamo trovare elementi c_i e d_i di A tali che $a_i = c_i a$ e $b_i = d_i b$, e quindi $x = \sum c_i a d_i b = (\sum c_i d_i) ab \in (ab)$. Se scegliamo $A = \mathbb{Z}$, $I = J = (2)$, allora $I \cap J = (2)$ ma $IJ = (2^2) = (4) \neq (2)$.

32) Sia γ un generatore di G, e sia φ un automorfismo di G; allora $\varphi(\gamma) = \gamma^k$ per qualche intero k. Dato che anche $\varphi(\gamma)$ deve essere un generatore di G, e quindi deve avere

periodo 18, k deve essere primo con 18. Inoltre, se $g = \gamma^h$ è un qualsiasi elemento di G, allora $\varphi(g) = \varphi(\gamma^h) = \gamma^{hk} = g^k$. Viceversa, se m è un intero primo con 18, $g \mapsto g^m$ definisce un automorfismo φ_m di G. Inoltre $\varphi_{m+18l}(g) = g^{m+18l} = g^m g^{18l} = g^m \mathbf{1} = g^m = \varphi_m(g)$; in altre parole, φ_m dipende solo dalla classe di congruenza di m modulo 18. Infine $\varphi_m(\varphi_n(g)) = \varphi_n(g)^m = (g^n)^m = g^{nm} = \varphi_{mn}(g)$, cioè $\varphi_m \circ \varphi_n = \varphi_{mn}$. Quello che si è mostrato finora è che $m \mapsto \varphi_m$ definisce un omomorfismo suriettivo dal gruppo moltiplicativo delle classi modulo 18 degli interi primi con 18 al gruppo degli automorfismi di G. Per vedere che questo omomorfismo è in realtà un isomorfismo basta ora vedere che è iniettivo. In effetti, se $\varphi_m = \varphi_n$, in particolare $\varphi_m(\gamma) = \varphi_n(\gamma)$, e quindi $\gamma^{m-n} = \mathbf{1}$; ne segue che $m - n$ deve essere divisibile per 18, cioè che le classi modulo 18 di m ed n coincidono. Osserviamo che in particolare segue da quanto detto che $\mathrm{Aut}(G)$ è abeliano. Notiamo ora che le classi di congruenza modulo 18 di interi primi con 18 sono quelle di 1, 5, 7, 11, 13 e 17. Dunque $\mathrm{Aut}(G)$ è un gruppo abeliano con 6 elementi, e quindi è ciclico. Un generatore di questo gruppo è φ_5. In effetti

$$\begin{aligned} 5 \cdot 5 = 25 &\equiv 7 \mod 18 \\ 5 \cdot 7 = 35 &\equiv 17 \mod 18 \\ 5 \cdot 17 \equiv 5 \cdot (-1) \equiv -5 &\equiv 13 \mod 18 \\ 5 \cdot 13 = 65 &\equiv 11 \mod 18 \end{aligned}$$

33) L'ordine di S_{10} è $10! = 5^2 k$, dove k è un intero primo con 5. Dunque, se H è un 5-sottogruppo di Sylow di S_{10}, H ha ordine $5^2 = 25$. Un gruppo il cui ordine sia il quadrato di un numero primo è necessariamente abeliano. Quindi, per il teorema di struttura dei gruppi abeliani, H può essere isomorfo al prodotto diretto di due gruppi ciclici di ordine 5 o può essere ciclico. Basta escludere la seconda possibilità. In effetti, se questa si verificasse, S_{10} dovrebbe contenere un elemento σ di ordine 25, il che è impossibile. Infatti, se $\sigma = \sigma_1 \cdots \sigma_n$ è la decomposizione di σ in prodotto di cicli disgiunti, dove l'ordine di σ_i è l_i e $\sum l_i = 10$, da $\sigma^{25} = \mathbf{1}$ segue che $\sigma_i^{25} = \mathbf{1}$ per ogni i, e dunque che $l_i \big| 25$ per ogni i. Dunque l_i può essere uguale a 1 o a 5 (non a 25 perchè non supera 10). Ne segue che $\sigma_i^5 = \mathbf{1}$, e quindi che $\sigma^5 = \mathbf{1}$, contro l'ipotesi.

34) Siano a e b elementi di X, e supponiamo per assurdo che $ab \notin X$. Questo significa che c'è $c \neq 0$ tale che $abc = 0$; dato che b non è un divisore di zero, e quindi $bc \neq 0$, questo dice che a è un divisore di zero, contro l'ipotesi. Sia ora u un elemento di U, e supponiamo che $uv = 0$ per qualche $v \in A$. Allora $0 = u^{-1}uv = v$. Ne segue che u non è un divisore di zero. Supponiamo ora che A sia finito, e sia x un elemento di X; bisogna mostrare che $x \in U$, cioè che x è invertibile. Si è già mostrato che, se $y \in X$, allora $xy \in X$. Dunque la moltiplicazione per x definisce una applicazione $\varphi : X \to X$. Se $y, z \in X$ e $\varphi(y) = \varphi(z)$, cioè se $xy = xz$, o, in altri termini, se $x(y - z) = 0$, si conclude che $y - z = 0$, cioè che $y = z$, dato che x non è un divisore di zero. Dunque φ è iniettiva, e quindi suriettiva, visto che X è un insieme finito. In particolare c'è un $y \in X$ tale che $xy = \mathbf{1}$; questo significa che x è invertibile.

35) a) è riducibile perchè è uguale a $(X^2+1)(X^2+X-1)$. b) è irriducibile per il criterio di Eisenstein; infatti i suoi coefficenti, tranne quello di grado massimo, sono divisibili per

3, ma il termine costante non è divisibile per 3^2. c) è anch'esso irriducibile. Infatti, se non lo fosse, avrebbe un fattore di grado 1, cioè avrebbe una radice, necessariamente intera. Questa radice dovrebbe dividere 25, e quindi sarebbe dispari. Ma se η è un intero dispari $\eta^3 + 6\eta^2 + 5\eta + 25$ è somma di tre interi dispari e di uno pari, e quindi non può essere nullo.

36) Indichiamo con b_i l'immagine di a_i in $F = A/M$. Dato che M è massimale, $F = K[b_1, \ldots, b_n]$ è un campo. Poiché F è finitamente generato su K, è algebrico su K. Dato che $\mathbb{C}$ è algebricamente chiuso, non è propriamente contenuto in alcun suo ampliamento algebrico; quindi, se $K = \mathbb{C}$, allora $F = \mathbb{C}$. Se invece $K = \mathbb{R}$, allora $F = \mathbb{R}$ o $F = \mathbb{C}$, dato che il solo ampliamento algebrico proprio di $\mathbb{R}$ è $\mathbb{C}$.

37) VERO. Infatti Q è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/6\mathbb{Z}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

38) Sia $\alpha : S_3 \to \mathrm{Aut}(S_3)$ l'omomorfismo che associa ad ogni $g \in S_3$ l'automorfismo interno $a \mapsto gag^{-1}$. Dico che α è un isomorfismo. In effetti, gli elementi non nulli di S_3 hanno ordine 2 o 3; se a ha ordine 2 e b ha ordine 3, allora $ab = b^{-1}a \neq ba$, e quindi a e b non commutano. Ciò implica che il nucleo di α, cioè il centro di S_3, è $\{1\}$, e dunque che α è iniettivo. Siano a_1, a_2 e a_3 gli elementi di ordine 2 di S_3, e sia f un automorfismo di S_3. Dato che, per ogni elemento g di S_3, $f(g)$ e g hanno lo stesso ordine, f permuta a_1, a_2, a_3. Se S è il gruppo delle permutazioni di a_1, a_2, a_3 questo dà un omomorfismo $\beta : \mathrm{Aut}(S_3) \to S$. Dato che S ha 6 elementi come S_3, per mostrare che α è suriettiva basta mostrare che β è iniettiva. Ma se $f(a_i) = a_i$ per $i = 1, 2, 3$, allora $f(a_1a_2) = f(a_1)f(a_2) = a_1a_2$, e analogamente $f(a_2a_1) = a_2a_1$. Dato che a_1a_2 e a_2a_1 sono i due elementi di ordine 3 di S_3, questo dice che f è l'identità.

39) FALSO: se $I \neq (0)$ e $J \neq (0)$, e i, j sono elementi non nulli di I e J, allora $(i, 1)$ e $(1, j)$ non appartengono a $I \times J$ ma $(i, 1)(1, j) = (i, j) \in I \times J$.

40) $A/(a) \simeq \mathbb{Z}/(p)[X]$ è un dominio di integrità perchè è un anello di polinomi su un campo. Anche $A/(b) \simeq \mathbb{Z}$ è un dominio di integrità. Quindi (a) e (b) sono ideali primi. Siano ora x e y elementi di A tali che $xy = 0$. In altre parole, se pensiamo x e y come classi di polinomi $P(X)$ e $Q(X)$, il prodotto PQ è divisibile per pX. Dunque PQ è divisibile anche per X, cioè non ha termine noto; dato che il termine noto di PQ è il prodotto di quelli di P e Q, uno dei due, diciamo quello di P, è nullo. In altre parole P è della forma $XR(X)$. Se scriviamo $PQ = pXS(X)$, ne ricaviamo che $pXS = XRQ$. Se usiamo il fatto che $\mathbb{Z}[X]$ è un dominio di integrità, possiamo concludere che $pS = RQ$. Scriviamo $R(X) = \sum a_i X^i$ e $Q(X) = \sum b_i X^i$. Vogliamo mostrare che p divide o R o Q. Supponiamo di no, e siano i e j gli indici piú piccoli con la proprietà che p non divide né a_i né b_j. Allora il coefficiente di pS di indice $i + j$ è $\sum_{h+k=i+j} a_h b_k$. In questa somma ogni termine è tale che $h < i$ o $k < j$, e quindi è divisibile per p, tranne $a_i b_j$. Questo però è in contraddizione con il fatto che tutti i coefficienti di pS sono ovviamente divisibili per p. Se p divide R, ne segue che pX divide P, e quindi $x = 0$. Altrimenti X divide P e p divide Q, cioè $x \in (a)$ e $y \in (b)$. Ciò significa che i divisori di zero di A appartengono ad (a) o a (b). D'altra parte gli elementi di $(a) \cup (b)$ sono tutti divisori di zero perchè $ab = 0$.

41) Se P non fosse irriducibile avrebbe un fattore di grado uno in $\mathbb{Z}_3[X]$, quindi avrebbe una radice in $\mathbb{Z}_3$. Però $P(0) = P(1) = P(-1) = 1$, quindi questo non accade. Visto che siamo in caratteristica 3, $(a+b)^3 = a^3 + b^3$ per ogni a e b. Quindi

$$P(\zeta \pm 1) = \zeta^3 \pm 1 - \zeta \mp 1 + 1 = P(\zeta) = 0\,.$$

Infine, dato che ζ, $\zeta + 1$ e $\zeta - 1$ sono distinti, non vi sono altre radici di P. Dato che $\zeta + 1$ e $\zeta - 1$ appartengono a $\mathbb{Z}_3[\zeta]$, questo è il campo di spezzamento di P su $\mathbb{Z}_3$. Il suo grado su $\mathbb{Z}_3$ è il grado del polinomio minimo di ζ, cioè di P, e vale quindi 3.

42) $\sigma = (1\ 7\ 8\ 5\ 4)(2\ 9\ 3) = (1\ 7)(7\ 8)(8\ 5)(5\ 4)(2\ 9)(9\ 3)$, $\tau = (1\ 3)(2\ 8\ 7)(4\ 5\ 6) = (1\ 3)(2\ 8)(8\ 7)(4\ 5)(5\ 6)$.

43) Supponiamo che $\zeta^n = 1$ e $\xi^m = 1$. Allora $\xi^{-m} = 1$, e quindi

$$(\zeta\xi^{-1})^{nm} = (\zeta^n)^m(\xi^{-m})^n = 1^m 1^n = 1.$$

Dunque, se $\zeta \in R$ e $\xi \in R$, allora $\zeta\xi^{-1} \in R$. Questo mostra che R è un sottogruppo.

44) Sia G un gruppo di ordine $153 = 3^2 \cdot 17$. Il numero dei 3-Sylow di G è della forma $1 + 3k$ e divide 17, quindi non può che essere 1, dato che 16 non è divisibile per 3. Il numero dei 17-Sylow di G è della forma $1 + 17k$ e divide 9, quindi non può che essere 1. Dunque G ha un solo 3-Sylow H e un solo 17-Sylow K, entrambi normali. Ne segue che G è prodotto diretto di H e K; dato che K è ciclico e H abeliano, in quanto il suo ordine è quadrato di un primo, anche G è abeliano. Il prodotto diretto di due gruppi ciclici di ordini 3 e 51 ha ordine 153 ma non è ciclico, perchè l'ordine di ogni suo elemento divide 51.

45) Sia $\alpha : G \to G/N$ il passaggio al quoziente, cosicché $H/N = \alpha(H)$. Se $g \in G$, allora $\alpha(gHg^{-1}) = \alpha(g)\alpha(H)\alpha(g)^{-1}$. I coniugati di H/N sono dunque le immagini tramite α dei coniugati di H. Dato che $H \supset N$, e che N è normale, ogni coniugato di H contiene N. Sappiamo che $L \mapsto \alpha(L)$ stabilisce una corrispondenza biunivoca tra sottogruppi di G contenenti N e sottogruppi di G/N; dunque questa applicazione stabilisce anche una corrispondenza biunivoca tra coniugati di H e coniugati di H/N.

46) Associamo ad ogni elemento g di G la permutazione di G/H che associa ad ogni laterale γH il laterale $g\gamma H$. Questo dà un omomorfismo $\alpha : G \to S(G/H) = S_3$; sia N il suo nucleo. I coniugati di H in G sono in corrispondenza biunivoca con quelli di $\alpha(H)$ in $\alpha(G)$. Se $\alpha(G)$ è diverso da $S(G/H)$, ha ordine al più 3, e dunque $H = N$ è normale, contro le ipotesi. Ne segue che α è suriettivo, e dunque $\alpha(H)$ ha ordine 2; i coniugati di $\alpha(H)$, e quindi anche quelli di H, sono 3.

47)

$$\sigma = (2\ 3)(1\ 8\ 4\ 6\ 5\ 7) = (2\ 3)(1\ 8)(8\ 4)(4\ 6)(6\ 5)(5\ 7)\,;$$
$$\tau = (1\ 3\ 4)(2\ 7\ 5)(6\ 8) = (1\ 3)(3\ 4)(2\ 7)(7\ 5)(6\ 8)\,.$$

48) Identifichiamo C_3 e C_7 ai sottogruppi di G costituiti da tutti gli elementi della forma $(x, 1)$ o, rispettivamente, $(1, y)$. Se φ è un automorfismo di G, allora $\varphi(C_3) = C_3$ e

$\varphi(C_7) = C_7$ perchè gli elementi non banali di C_3 hanno ordine 3 e quelli non banali di C_7 hanno ordine 7. Gli automorfismi di G sono dunque tutte e sole le applicazioni $\varphi : C_3 \times C_7 \to C_3 \times C_7$ della forma $\varphi(x, y) = (f(x), g(y))$, dove f e g sono automorfismi di C_3 e di C_7. In altre parole, $\mathrm{Aut}(G)$ è il prodotto diretto di $\mathrm{Aut}(C_3)$ e $\mathrm{Aut}(C_7)$, che sono ciclici di ordini 2 e 6. Quindi $\mathrm{Aut}(G)$ è abeliano di ordine 12 ma non è ciclico, in quanto il prodotto di due gruppi ciclici è ciclico se e solo se gli ordini dei due fattori sono primi fra loro.

49) Sia G un gruppo di ordine $1225 = 5^2 7^2$. Il numero dei 5-Sylow divide 7^2 ed è della forma $1 + 5k$, quindi non può essere che 1. Il numero dei 7-Sylow divide 5^2 ed è della forma $1 + 7k$, quindi anch'esso non può essere che 1. Poiché vi sono un solo 5-Sylow e un solo 7-Sylow, questi sono normali e G ne è prodotto diretto. D'altra parte, dato che ogni gruppo il cui ordine sia il quadrato di un primo è abeliano, il 5-Sylow e il 7-Sylow sono abeliani. Quindi anche G è abeliano, in quanto prodotto diretto di gruppi abeliani.

50) Supponiamo che ogni elemento di $A - I$ sia invertibile. Dato che un ideale che contenga un elemento invertibile deve coincidere con A, ogni ideale proprio non ha elementi in comune con $A - I$, cioè è contenuto in I. Viceversa, se ogni ideale proprio è contenuto in I, allora l'ideale generato da un qualsiasi elemento $u \in A - I$ non può essere proprio, e quindi in particolare contiene 1. Questo significa che c'è un $v \in A$ tale che $uv = 1$; u è quindi invertibile. Se infine A è euclideo, e quindi a ideali principali, sia t un generatore di I. Ogni elemento primo di A genera un ideale massimale, che deve essere contenuto in I e quindi coincidere con I. Quindi ogni primo in A è associato a t. Se ora J è un ideale di A e s un suo generatore, s è associato a un prodotto di primi, quindi a t^k per qualche k. Questo significa che J è generato da t^k.

51) Il polinomio $P(X)$ è riducibile. Infatti $7^3 = 343 = 31 \cdot 11 + 2$, quindi 7 è una radice di P modulo 11. Dunque I non è primo e quindi $A = K[X]/I$ non è un dominio; in particolare, non è un campo. Sia B un elemento di $K[X]$. Possiamo scrivere, e in modo unico, $B = QP + R$, dove $Q, R \in K[X]$ e R ha grado al più 2. In altre parole, vi è una corrispondenza biunivoca tra i polinomi di grado al più due a coefficienti in K e gli elementi di A. Un polinomio di grado al più 2 è determinato dalla terna dei suoi coefficienti. Dato che vi sono $11^3 = 1331$ terne possibili, altrettanti sono gli elementi di A.

52) Le decomposizioni in cicli disgiunti di α, β e γ sono

$$\alpha = (1\ 6\ 3)(2\ 5)(7\ 8\ 9)$$
$$\beta = (1\ 7)(2\ 6\ 4\ 3\ 5\ 8)$$
$$\gamma = (1\ 2\ 5\ 4)(3\ 7\ 9\ 8)$$

Dato che i cicli di lunghezza pari sono permutazioni dispari e quelli di lunghezza dispari sono permutazioni pari, α è dispari mentre β e γ sono pari.

53) Se $(a, b) \in G \times S_3$ è tale che $(a, b)(g, s) = (g, s)(a, b)$, deve essere $ag = ga$ e $bs = sb$. Dunque (a, b) appartiene al centro di $G \times S_3$ se e solo se a appartiene al centro di

G e b a quello di S_3. Il centro di S_3 è $\{1\}$. Quanto al centro di G, questo gruppo è generato da σ e ρ, dove σ ha ordine 2, ρ ha ordine 6 e $\rho^h\sigma = \sigma\rho^{6-h}$. Gli elementi di G sono $1, \rho, \rho^2, \ldots, \rho^5$ e $\sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^5$ Si ha che $\rho^h(\sigma\rho^n) = (\sigma\rho^n)\rho^{6-h}$, quindi $\sigma\rho^n$ non appartiene al centro di G per alcun n. Invece ρ^n appartiene al centro si G se e solo se commuta con σ, cioè se e solo se $n = 3$. Quindi il centro di G è $\{1, \rho^3\}$.

54) $56 = 2^3 7$. Il numero dei 7-sottogruppi di Sylow è della forma $1 + 7k$ e divide 8, quindi può essere 1 o 8. Nel primo caso vi è un unico 7-sottogruppo di Sylow, che è normale. Nel secondo caso due qualsiasi 7-sottogruppi di Sylow distinti hanno come intersezione $\{1\}$, per il teorema di Lagrange e perchè 7 è primo. Quindi vi sono nel gruppo $8 \cdot 6 = 48$ elementi di ordine 7, nessuno dei quali può appartenere a un 2-sottogruppo di Sylow. Restano 8 elementi quindi vi è un unico 2-sottogruppo di Sylow, che è il complementare dell'insieme degli elementi di ordine 7; è normale perchè unico.

55) Se $a + b\sqrt{2} = c + d\sqrt{2}$ allora $a = c$, $b = d$, altrimenti si potrebbe concludere che $\sqrt{2}$ è razionale. Se poi $z = a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + a_3\sqrt{2}^3 + \cdots$ è un elemento di A, lo possiamo anche scrivere come $a_0 + 2a_2 + \cdots + (a_1 + 2a_3 + \cdots)\sqrt{2}$. L'applicazione φ è biunivoca perchè $\varphi \circ \varphi = \mathbf{1}$. È chiaro che $\varphi(z + w) = \varphi(z) + \varphi(w)$. Poi

$$\varphi((a + b\sqrt{2})(c + d\sqrt{2})) = \varphi(ac + 2bd + (ad + bc)\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2}\,,$$
$$\varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2}) = (a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2}\,.$$

Notiamo che $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, che è intero. Poi

$$N(zw) = zw\varphi(zw) = zw\varphi(z)\varphi(w) = N(z)N(w)\,.$$

Notiamo anche che $N(1) = 1$. Supponiamo che z sia invertibile, cioè che ci sia w tale che $zw = 1$. Allora $1 = N(1) = N(zw) = N(z)N(w)$, cioè $N(z)$ è un intero invertibile, e quindi uguale a ± 1. Viceversa, dire che $N(w) = \pm 1$ equivale a dire che $z\varphi(z) = \pm 1$, e quindi che $\pm\varphi(z)$ è un inverso di z in A.

56) Poniamo $A = \mathbb{Z}[X]$. Bisogna mostrare che A/I è un campo. Scriviamo $A/I = (A/5A)/(I/5A)$; dobbiamo quindi mostrare che $I/5A$ è massimale in $A/5A = \mathbb{Z}_5[X]$, cioè, dato che Z_5 è un campo, che è primo. Però $I/5A$ è l'ideale generato da P, visto come polinomio a coefficienti in $\mathbb{Z}_5$. Bisogna quindi vedere che P è irriducibile in $\mathbb{Z}_5[X]$, cioè, dato che ha grado 3, che non ha radici in $\mathbb{Z}_5$. Facendo i conti si vede che, modulo 5, $P(0) \equiv 1$, $P(1) \equiv -1$, $P(2) \equiv -3$, $P(3) \equiv 1$, $P(4) \equiv= -3$.

57) Sia σ un elemento di S_7. σ è un prodotto di cicli disgiunti la somma delle cui lunghezze non supera 7; siano $l_1 \geq l_2 \geq l_3 \geq \cdots$ le lunghezze di questi cicli. Le possibilità per

queste lunghezze e gli ordini delle corrispondenti permutazioni sono

7	7
6	6
5	5
4	4
3	3
2	2
5, 2	10
4, 3	12
4, 2	4
3, 3	3
3, 2	6
2, 2	2
3, 2, 2	6
2, 2, 2	2

Dunque gli ordini possibili sono 1, 2, 3, 4, 5, 6, 7, 10, 12.

58) $55 = 5 \cdot 11$ è prodotto di due primi. Quindi un gruppo G di ordine 55 contiene un unico 11-sottogruppo di Sylow, che è normale; lo indichiamo con H, e indichiamo con K un 5-sottogruppo di Sylow. Il numero dei 5-Sylow è congruo a 1 modulo 5 e divide 11; può quindi essere 1 o 11. Nel primo caso K è normale e quindi G è prodotto diretto di H e K. Dato che questi due gruppi hanno ordine primo, sono ciclici. Dato che hanno ordini primi fra loro anche G è ciclico. Supponiamo che K non sia normale. Allora G è il prodotto semidiretto di H e K corrispondente all'omomorfismo $K \xrightarrow{\alpha} \mathrm{Aut}(H)$ indotto dal coniugio. Questo omomorfismo non può essere banale dato che stiamo supponendo K non normale; dato che K non ha sottogruppi propri non banali, deve essere iniettivo. Il gruppo degli automorfismi di H è ciclico di ordine 10, e contiene un solo sottogruppo di ordine 5. L'omomorfismo α è dato da un qualsiasi isomorfismo tra questo gruppo e K. Dato che, a meno di automorfismi di K, vi è un unico tale isomorfismo, vi è un unico gruppo non abeliano di ordine 55.

59) Vero: sia p un numero primo, e sia G un gruppo non abeliano di ordine p^3 (ad esempio un gruppo non abeliano di ordine 8). Dato che G è un p-gruppo il suo centro Z non è banale. Quindi G/Z ha ordine p o p^2 (in effetti, ordine p^2), e quindi deve essere abeliano.

60) Se $a, b \in M$ non sono nulli, e $a + b \neq 0$, allora $d(a + b) \geq \min(d(a), d(b)) > d(1)$. Se $a \in M$ e $b \in A$ non sono nulli, allora $d(ab) \geq d(a) > d(1)$. Questo mostra che M è un ideale. Mostriamo che gli elementi di $A - M$ sono invertibili. Intanto, se $a \neq 0$, $d(a) = d(a \cdot 1) \geq d(1)$. Se $d(a) = d(1)$ la divisione con resto di 1 per a dà $1 = qa + r$, dove $r = 0$ oppure $d(r) < d(a) = d(1)$. Questa seconda alternativa è impossibile, e quindi a è invertibile.

61) In quello che segue tutte le congruenze si intendono modulo 5. $P(0) = -4 \not\equiv 0$, $P(1) = -4 \not\equiv 0$, $P(2) = 0$, $P(0) = 14 \not\equiv 0$, $P(0) = 44 \not\equiv 0$. Dividendo per $X - 2$

si ottiene che $P(X) = (X-2)(X^2+X+2)$. Inoltre $2^2+2+2 = 8 \not\equiv 0$, quindi X^2+X+2 non ha radici in $\mathbb{F}_5$ ed è irriducibile. Ne segue che $K = \mathbb{F}_5[\alpha]$, dove α è una radice di X^2+X+2, che $[K:\mathbb{F}_5] = 2$, e quindi che il numero di elementi di K è $5^2 = 25$. Mostriamo che X^2-2 ha radici in K. Poiché $\mathbb{F}_5^\times$ ha ordine 4, le quarte potenze dei suoi elementi valgono tutte 1. Il gruppo moltiplicativo di K è ciclico di ordine 24, e quindi contiene un unico sottogruppo di ordine 4, che consiste di tutti e soli gli elementi g tali che $g^4 = 1$ o, che è lo stesso, di tutte le seste potenze di elementi di $K^\times$. Dunque tutti gli elementi di $\mathbb{F}_5^\times$, e quindi in particolare 2, sono quadrati di elementi di K.

62) La decomposizione in cicli di σ è (1 2)(3 4 5). Le orbite di σ sono dunque $X = \{1,2\}$ e $Y = \{3,4,5\}$. Supponiamo che $\rho\sigma = \sigma\rho$. Allora $\rho(X) = \rho\sigma(X) = \sigma\rho(X)$, quindi $\rho(X)$ è un'orbita di σ; poiché ha due elementi e Y ne ha tre, deve essere X. Allo stesso modo si mostra che $\rho(Y) = Y$. La restrizione di ρ a Y deve commutare con (3 4 5), e quindi deve essere una permutazione ciclica di $\{3,4,5\}$. Le permutazioni cercate sono quindi tutte e sole quelle della forma $\alpha^i\beta^j$, dove $\alpha = (1\ 2)$ e $\beta = (3\ 4\ 5)$.

63) G è generato da due elementi α e β di ordini, rispettivamente, k e 2, tali che $\alpha\beta = \beta\alpha^{-1}$. Sia H il sottogruppo generato da α e sia K un suo sottogruppo. Se $\alpha^i \in K$ allora

$$\alpha^j\beta\alpha^i(\alpha^j\beta)^{-1} = \alpha^j\beta\alpha^i\beta\alpha^{-j} = \alpha^j\beta\beta\alpha^{-i-j} = \alpha^{j-i-j} = \alpha^{-i} \in K\,,$$

quindi K è normale. Supponiamo invece che K sia un sottogruppo normale non contenuto in H; necessariamente K contiene un elemento $\alpha^j\beta$. Allora

$$\alpha^{2i+j}\beta = \alpha^i(\alpha^j\beta)\alpha^{-i} \in K$$

e quindi $\alpha^{2i} \in K$ per ogni i. Se k è dispari ogni elemento di H è della forma α^{2i}, e quindi $K = G$. Invece se k è pari K può anche essere il sottogruppo Γ_j di indice due generato da α^2 e $\alpha^j\beta$.

64) $80 = 5\cdot 2^4$. Se G è un gruppo di ordine 80 il numero dei suoi 5-Sylow è della forma $1+5k$ e divide 16; può quindi essere 1 o 16. Se vi è un solo 5-Sylow, è normale, e quindi G non è semplice. Supponiamo che i 5-Sylow siano 16; dato che l'intersezione tra due distinti 5-Sylow è ridotta al solo elemento neutro, vi sono $16\cdot 4 = 64$ elementi di ordine 5. Detto altrimenti, vi sono 16 elementi che non hanno ordine 5. Dato che un 2-Sylow ha ordine 16 e i suoi elementi non hanno ordine 5 vi è un solo 2-Sylow, che è quindi normale. Dunque G non è semplice.

65) Gli ideali propri di $\mathbb{Z}_{45} = \mathbb{Z}/45\mathbb{Z}$ sono tutti della forma $I/45\mathbb{Z}$, dove I è un ideale proprio di $\mathbb{Z}$ contenente $45\mathbb{Z}$, cioè della forma $k\mathbb{Z}/45\mathbb{Z}$, dove $k|45$ e $k \neq \pm 1$; inoltre un tale ideale è primo, o massimale, se e solo se lo è $k\mathbb{Z}$. I valori possibili di k sono dunque $3, 9, 5, 15, 45$, corrispondente quest'ultimo all'ideale 0. I valori corrispondenti a ideali primi o, che è lo stesso, massimali, sono 3 e 5.

66) Sia x un elemento non nullo di $\mathbb{F}_{3^h}$. Allora $x^{3^h-1} = 1$; se $h = 1,2,3$, allora 3^h-1 è uguale, rispettivamente, a $2, 8, 26$. Questi tre numeri sono primi con 5; quindi, se

poniamo $\gamma = 3^h - 1$, ci sono interi a e b tali che $1 = a\gamma + 5b$. Ne segue che, se $x^5 = 1$, allora $x = x^1 = x^{a\gamma+5b} = (x^\gamma)^a(x^5)^b = 1$. Una radice di $X^5 - 1$ è ovviamente 1. Dividendo per $X - 1$ si ricava che $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Inoltre 1 non è radice di $X^4 + X^3 + X^2 + X + 1$. Sia ζ una radice di $X^4 + X^3 + X^2 + X + 1$. Le radici quinte non banali di 1 sono ζ, ζ^2, ζ^3, ζ^4, quindi il campo di spezzamento di $X^5 - 1$ è $K = \mathbb{F}_3[\zeta]$. Il campo K ha ordine 3^h, dove h è il grado del polinomio minimo di ζ. Dato che ζ è radice di un polinomio di grado 4, $h \leq 4$. Però K contiene radici non banali di 1, e quindi $h \geq 4$. In definitiva l'ordine di K è 3^4, e quindi $[K : \mathbb{F}_3] = 4$.

67) Se $\sigma(\{1,2\}) = \{1,2\}$ e $\tau(\{1,2\}) = \{1,2\}$, allora $\tau^{-1}(\{1,2\}) = \{1,2\}$ e $\sigma\tau^{-1}(\{1,2\}) = \sigma(\{1,2\}) = \{1,2\}$. Questo mostra che G è un sottogruppo di S_5. La restrizione a $\{1,2\}$ dà un omomorfismo (suriettivo) da G a S_2. Il nucleo di questo omomorfismo è costituito da tutte le permutazioni che fissano 1 e 2, e si identifica quindi alle permutazioni di $\{3,4,5\}$, e dunque a S_3. L'ordine di G è perciò $\#(S_3)\#(S_2) = 12$.

68) Se G è abeliano, non c'è niente da dimostrare. Supponiamo quindi che G non sia abeliano. Dato che G è un p-gruppo, con $p = 3$, il suo centro Z non è banale. Inoltre H è abeliano, in quanto ha ordine p^2. Sia g un elemento non banale di Z. Supponiamo che g non appartenga a H. Dato che si trova nel centro di G, commuta con tutti gli elementi di G, e in particolare con quelli di H. Dunque il sottogruppo generato da H e da g è abeliano. Dato che è strettamente più grande di H, e H ha indice p, deve coincidere con G. Si conclude che G è abeliano, in contraddizione con quanto supposto.

69) Sia a un elemento di $K[X]$, algebrico su K. L'algebricità di a implica che $K[a]$ è un campo. In particolare a, se non è nullo, è invertibile in $K[X]$. Sappiamo però che gli elementi invertibili di questo anello sono i polinomi di grado zero non nulli, cioè gli elementi di $K^\times$. Ne segue che a è un elemento di K.

70) a) Siano $\overline{a_1}, \ldots, \overline{a_n}$ le classi di resti di $a_1, \ldots, a_n$ modulo M. Dato che M è massimale, l'anello

$$A/M = \mathbb{R}[\overline{a_1}, \ldots, \overline{a_n}]$$

è un campo. Ne segue che $\overline{a_1}, \ldots, \overline{a_n}$ sono algebrici su $\mathbb{R}$, e quindi A/M è una estensione algebrica di $\mathbb{R}$. Visto che $\mathbb{C}$ è algebricamente chiuso ("teorema fondamentale dell'algebra") e algebrico su $\mathbb{R}$, A/M può essere identificato a un sottocampo di $\mathbb{C}$ contenente $\mathbb{R}$. Poiché $\mathbb{C}$ ha grado 2 su $\mathbb{R}$, A/M deve essere uguale a $\mathbb{R}$ o a $\mathbb{C}$.
b) $A = \mathbb{R}[X]$, dove X è una indeterminata. Se M è l'ideale generato da $X - 1$, allora $A/M \simeq \mathbb{R}$. Se M è l'ideale generato da $X^2 + 1$, allora $A/M = \mathbb{R}[i] = \mathbb{C}$.