Algebra 1 – Matematica – A.A. 2022-23, corso annuale
Docente: Alberto De Sole

Esercizi

MODULO 1

Teoria della cardinalità. Lemma di Zorn.

Ex.1 - Dimostrare che LZ $\Rightarrow$ AS. Suggerimento: dato un insieme $X \neq \emptyset$, si consideri l'insieme

$$\mathcal{S} = \left\{ (\mathcal{F}, f) \,\middle|\, \mathcal{F} \subset \mathcal{P}(X),\ f : \mathcal{F} \to X \text{ funzione di scelta} \right\},$$

con la relazione d'ordine $(\mathcal{F}, g) < (\mathcal{G}, g)$ se

$$\mathcal{F} \subset \mathcal{G}\ , \qquad g|_{\mathcal{F}} = f\,.$$

Far vedere che valgono le ipotesi del Lemma di Zorn ed usare la tesi del Lemma di Zorn per costruire una funzione di scelta su X.

Ex.2 - Se A è un insieme infinito ed $n \in \mathbb{N}$, dimostrare che $|A^n| = |A|$.

Ex.3 - Dati insiemi infiniti $A_1, \dots, A_n$ con $|A_1| \leq |A_2| \leq \cdots \leq |A_n|$, dimostrare che $|A_1 \times \cdots \times A_n| = |A_n|$.

Ex.4 - Dare un esempio di applicazinoi $f : X \to X$ e $g : X \to X$ non invertibili tali che $g \circ f = \mathbb{1}_X$.

Ex.5 - Mostrare che ogni funzione $f : X \to Y$ si può esprimere nella forma $f = g \circ h$ dove $h : X \to Z$ è iniettiva e $g : Z \to Y$ è suriettiva.

Ex.6 - Mostrare che ogni funzione $f : X \to Y$ si può esprimere nella forma $f = g \circ h$ dove $h : X \to Z$ è suriettiva e $g : Z \to Y$ è iniettiva.

Ex.7 - Sia X un insieme infinito e sia $\mathcal{P}^{\text{fin}}(X)$ l'insieme dei sottoinsiemi finiti di X. Mostrare che $|\mathcal{P}^{\text{fin}}(X)| = |X|$.

Ex.8 - Mostrare che se $\mathbb{K}$ è un campo infinito e V è uno spazio vettoriale su $\mathbb{K}$ con dimensione al più numerabile, allora $|V| = |\mathbb{K}|$.

Ex.9 - Sia V uno spazio vettoriale sul campo $\mathbb{K}$ con base $\mathcal{B}$. Mostrare che se $\mathbb{K}$ e $\mathcal{B}$ sono infiniti, allora $|V| = \max\{|\mathbb{K}|, |\mathcal{B}|\}$.

Ex.10 - Denotiamo con X^Y l'insieme delle funzioni $f : Y \to X$. Fornire corrispondenze biunivoche $X^{Y \sqcup Z} \simeq X^Y \times X^Z$ e $(X^Y)^Z \simeq X^{Y \times Z}$.

Aritmetica.

Ex.1 - Siano $a, m, n \in \mathbb{N}$ con $a > 1$. Mostrare che se $MCD(m, n) = d$, allora $MCD(a^m - 1, a^n - 1) = a^d - 1$.

Ex.2 - Siano $a, m, n \in \mathbb{N}$ con $a > 1$. Mostrare che $a^m - 1$ divide $a^n - 1$ se e solo se m divide n.

Ex.3 - Mostrare che se $2^n - 1$ è primo allora n è primo.

Ex.4 - Siano $a > 1, n > 1$ interi. Mostrare che se $a^n - 1$ è primo, allora $a = 2$ e n è primo.

Ex.5 - Siano $a > 1, n > 1$ interi. Mostrare che se $a^n + 1$ è primo, allora a è pari e n è ua potenza di 2.

Ex.6 - La successione di Fibonacci F_n, $n \geq 1$ è definita ricorsivamente da $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ se $n \geq 2$. Calcolare $\text{MCD}(F_{10}, F_9)$ eseguendo l'algoritmo euclideo.

Ex.7 - Dimostrare che se p è primo e $p \equiv 1\,(4)$, allora $\left(\frac{p-1}{2}!\right)^2 \equiv -1\,(p)$.

Ex.8 - Calcolare l'idetità di Bezout per $3 = \text{MCD}(54321, 12345)$.

Ex.9 - Mostrare che per ogni $n \geq 1$ vale $\text{MCD}(n^2 - n + 1, n + 1)$ è 1 o 3.

Ex.10 - (a) Risolvere l'equazione alle congruenze $112x \equiv 223\,(335)$. (b) Risolvere l'equazione alle congruenze $112x \equiv 222\,(346)$.

Ex.11 - Calcolare l'inverso, se esiste, di $[123]$ in $\mathbb{Z}/2345$.

Ex.12 - Trovare tutte le soluzioni $x \in \mathbb{Z}$ dei seguenti sistemi alle congruenze:

$$\text{(a)} \begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}, \qquad \text{(b)} \begin{cases} 2x \equiv 1 \mod 5 \\ 4x \equiv 1 \mod 7 \\ 7x \equiv 1 \mod 11 \end{cases}, \qquad \text{(c)} \begin{cases} x \equiv 2 \mod 4 \\ x \equiv 4 \mod 6 \\ x \equiv 6 \mod 8 \end{cases}$$

Teoria dei gruppi: nozioni preliminari.

Ex.1 - Supponiamo che in un gruppo valga l'equazione $xyz = 1$. È vero che $yzx = 1$? È vero che $yxz = 1$?

Ex.2 - Sia G un gruppo con prodotto $\cdot$. Definiamo il *gruppo opposto* G° come l'insieme G dotato del prodotto opposto $a \circ b = b \cdot a$.
(a) Dimostrare che G° è un gruppo.
(b) Trovare un isomorfismo tra G e $^\circ$.

Ex.3 - Siano a, b elementi di un gruppo. Assumendo che a ha ordine 5 e $a^3b = ba^3$, mostrare che $ab = ba$.

Ex.4 - (a) Se un elemento $x \in G$ ha ordine rs, qual'è l'ordine di x^r?
(b) Se un elemento $x \in G$ ha ordine n, qual'è l'ordine di x^r?

Ex.5 - Dimostrare che se ogni elemento $x \in G$ diverso dall'unità ha ordine 2, allora G è abeliano.

Ex.6 - Determinare il gruppo degli automorfismi (= isomorfismi $\varphi : G \to G$) dei seguenti gruppi:
(a) $\mathbb{Z}, +$;
(b) gruppo ciclico di ordine 10;
(c) S_3.

Ex.7 - Descrivere tutti gli omomorfismi di gruppo $\mathbb{Z} \to \mathbb{Z}$, dicendo quali sono iniettivi, quali suriettivi e quali isomorfismi.

Ex.8 - Si consideri la funzione $f : \mathbb{R} \to \mathbb{C}^\times$, data da $f(x) = e^{ix}$. Mostrare che f è un omomorfismo di gruppi. Determinarne nucleo e immagine.

Ex.9 - Si consideri il gruppo additivo $\mathbb{R}^n$. Sia $W \subset \mathbb{R}^n$ il sottogruppo che consiste delle soluzioni di un sistema di equazioni lineari omogeneo $AX = 0$ (dove A è una matrice $m \times n$ fissata). Mostrare che l'insieme delle soluzioni di un sistema non omogeneo $AX = b$ è una classe laterale di W.

Ex.10 - (a) Mostrare che un sottogruppo $H \subset G$ di indice 2 (ovvero t.c. $|G/H| = 2$) è necessariamente normale.
(b) Far vedere con un esempio che un sottogruppo di indice 3 non è necessariamente normale.

Ex.11 - Siano a, b elementi di un gruppo G. Mostrare che ab e ba hanno lo stesso ordine.

Ex.12 - Mostrare con un esempio che il prodotto di elementi di ordine finito in un gruppo può non avere ordine finito. Che succede se il gruppo è abeliano?

Ex.13 - Mostrare che l'intersezione $H \cap K$ di sottogruppi di un gruppo G è un sottogruppo di H e che se K è un sottogruppo normale di G, allora $H \cap K$ è un sottogruppo normale di H.

Ex.14 - Sia H il sottogruppo ciclico, generato dalla permutazione $(1\,2\,3)$, del gruppo alterno A_4. Elencare le classi laterali sinistre e destre di H esplicitamente.

Ex.15 - Un gruppo di ordine 35 contiene necessariamente un elemento di ordine 5? E di ordine 7?

Ex.16 - Siano H, K sottogruppi di indice finito di G. Dimostrare che anche $H \cap K$ ha indice finito in G. Mostrare con un esempio che l'indice di $H \cap K$ in H non divide necessariamente l'indice di K in G.

Ex.17 - Sia G un gruppo di ordine pari. Dimostrare che esiste un elemento $a \in G$ di ordine 2.

Ex.18 - Sia G un insieme con un prodotto associativo $\cdot$ che soddisfa le seguenti condizioni:
(i) Esiste $e \in G$ tale che $a \cdot e = a$ per ogni $a \in G$.
(ii) Dato $a \in G$, esiste $y(a) \in G$ tale che $a \cdot y(a) = e$.
Dimostrare che $(G, \cdot)$ è gruppo.

Ex.19 - Sia G un insieme con un prodotto associativo $\cdot$ che soddisfa le seguenti condizioni:
(i) Esiste $e \in G$ tale che $a \cdot e = a$ per ogni $a \in G$.
(ii) Dato $a \in G$, esiste $y(a) \in G$ tale che $y(a) \cdot a = e$.
Far vedere con un esempio che $(G, \cdot)$ non è necessariamente un gruppo.

Ex.20 - Sia G un insieme finito con un prodotto associativo $\cdot$ per cui valgono entrambe le leggi di cancellazione $a \cdot b = a \cdot c \Rightarrow b = c$ e $a \cdot c = b \cdot c \Rightarrow a = b$. Dimostrare che $(G, \cdot)$ è un gruppo. Far vedere con un esempio che se vale una sola legge di cancellazione G non è necessariamente un gruppo. E far vedere con un esempio che, se G non è finito, non è necessariamente un gruppo anche se valgono entrambe le leggi di cancellazione.

Teoria dei gruppi: seconda parte.

(1) Si consideri il gruppo dei quaternioni $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ con prodotto dato dalle relazioni $i^2 = j^2 = k^2 = -1$, $ij = -ji = k, jk = -kj = i, k- = -ik = j$. Elencare tutti i sottogruppi di Q_8 e specificare quali siano normali.
(2) Individuare le classi di coniugio nel gruppo diedrale D_6 di ordine 12.
(3) Individuare le classi di coniugio nel gruppo diedrale D_7 di ordine 14.
(4) Descrivere le classi di coniugio nei gruppi S_6 e A_6.
(5) Sia $U \subset \mathrm{GL}_3(\mathbb{F}_3)$ il sottogruppo delle matrici triangolari superiori unipotenti (cioè con tutti 1 sulla diagonale) con coefficienti nel campo finito $\mathbb{F}_3$. Calcolare l'ordine di U, individuarne il centro e mostrare che ogni suo elemento diverso dall'identità ha ordine 3.
(6) Se $V = \{\mathbb{1}, (12)(34), (13)(24), (14)(23)\}$, mostrare che $V \subset S_4$ è un sottogruppo normale di S_4 e dimostrare che il quoziente S_4/V è isomorfo a S_3.
(7) Mostrare che il gruppo dei quaternioni Q_8 (cf. Esercizio 1) non è prodotto diretto nè prodotto semidiretto di due suoi sottogruppi propri.
(8) Mostrare che A_4 non possiede sottogruppi di ordine 6.
(9) Esibire tutti i sottogruppi di S_4 di ordine 8.
(10) Mostrare che, in un gruppo di ordine 12, almeno un sottogruppo di Sylow (ovvero di ordine 3 o 4) è normale.
(11) Se $|G| = m, |H| = n$ e $\mathrm{MCD}(m, n) = 1$, mostrare che l'unico omomorfismo $f : G \to H$ manda ogni elemento di G nell'identità di H.
(12) Descrivere tutti gli omomorfismi $A_4 \to D_4$.
(13) Descrivere tutti gli omomorfismi $A_4 \to S_3$.
(14) Un sottogruppo $H \subset G$ si dice *caratteristico* quando $\phi(H) = H$ per ogni scelta di $\phi \in \mathrm{Aut}(G)$.
- Mostrare che ogni sottogruppo caratteristico è normale.
- Dare un esempio di un sottogruppo normale che non sia caratteristico.
- Mostrare che $Z(G)$ è un sottogruppo caratteristico di G.
- Mostrare che un p-sottogruppo di Sylow è normale se e solo se è caratteristico.

(15) Mostrare che il prodotto semidiretto $N \rtimes_\phi H$ è abeliano se e solo se N, H sono abeliani e $\phi : H \to \mathrm{Aut}(N)$ manda ogni elemento di H in $\mathbb{1}_N$.
(16) Mostrare che se $p < q$ sono primi e p non divide $q - 1$ allora un gruppo di ordine pq è necessariamente ciclico.
(17) Classificare, a meno di isomorfismo, tutti i gruppi di ordine 12.
(18) Classificare, a meno di isomorfismo, tutti i gruppi di ordine 18.
(19) Costruire, come prodotto semidiretto, un gruppo non abeliano di ordine 39.
(20) Nel prodotto semidiretto $\overline{G} = N \rtimes_\phi H$ consideriamo i sottoinsiemi $\overline{H} = \{(1, h) \mid h \in H\}$ e $\overline{N} = \{(n, 1) \mid n \in N\}$. Mostrare che
- $\overline{H}$ e $\overline{N}$ sono sottogruppi di $\overline{G}$, isomorfi a H, N rispettivamente;
- $\overline{N}$ è un sottogruppo normale di $\overline{G}$;
- $\overline{N} \cap \overline{H} = \{(1, 1)\}$;
- $\overline{N} \cdot \overline{H} = \overline{G}$

- $(1,h)(n,1)(1,h)^{-1} = (\phi_h(n),1)$.

In altre parole, $\overline{G}$ è prodotto semidiretto dei suoi sottogruppi $\overline{N}, \overline{H}$ e ϕ descrive il modo in cui gli elementi di $\overline{H}$ coniugano quelli di $\overline{N}$.

MODULO 2

Teoria degli anelli

(1) (Herstein 3.2.7) Dare un sempio di un domonio di integrità a caratteristica finita con un numero infinito di elementi.
(2) (Herstein 3.2.9) Sia A un insieme che soddisfa tutti gli assiomi di anello commutativo con unità con l'eccezione della commutatività della somma. Mostrare allora che la somma è commutativa calcolando $(1+1)(x+y)$ in due modi diversi.
(3) (Herstein 3.4.3) Dimostrare che un omomorfismo non nullo $\phi : \mathbb{K} \to A$ da un campo $\mathbb{K}$ ad un anello A è necessariamente iniettivo.
(4) (Herstein 3.4.12) Si consideri l'anello A (non commutativo) delle matrici 2×2 a coefficienti razionali. Mostrare che gli unici ideali bilateri di A sono 0 e A.
(5) (Herstein 3.4.18) Sia A un anello, sia $I \subset A$ un ideale sinistro, e sia $r(I) = \{x \in A \,|\, xi = 0 \,\forall i \in I\}$. Mostrare che $r(I)$ è un ideale bilatero di A.
(6) (Herstein 3.6.5) Sia A un anello commutativo con unità. Sia $S \subset A$ un sottoinsieme *moltiplicativo*, ovvero tale che: (i) $0 \notin S$; (ii) $s,t \in S$ implica $st \in S$. Definire su $A \times S$ la seguente relazione di equivalenza: $(a,s) \simeq (b,t)$ se esiste $v \in S$ tale che $v(at-bs) = 0$. Dimostrare che si tratta di una relazione di equivalenza, e che nell'insieme quoziente $A_S := (A \times S)/\sim$ si può definire in modo canonico una struttura di anello (in modo analogo a quanto fatto per il campo delle frazioni di un dominio). Definire (in modo naturale) un omomorfismo $\varphi : A \to A_S$, verificare che $S \cap \ker\varphi = \emptyset$ e le immagini degli elementi di S in A_S sono invertibili.
(7) Sia A un anello commutativo con unità e siano I, J ideali di A. mostrare che: (i) $IJ = \{\sum_\alpha i_\alpha j_\alpha$ (somme finite) $\,|\, i_\alpha \in I,\, j_\alpha \in J\}$ è un ideale di A; (ii) $I \cap J$ è un ideale di A; (iii) $I + J = \{i + j \,|\, i \in I,\, j \in J\}$ è un ideale di A. (iv) Mostrare che $IJ \subset I \cap J$. Mostrare che, se $I + J = A$, allora: (v) $IJ = I \cap J$; (vi) vale il Teorema cinese dei resti: per ogni scelta di $a, b \in A$ esiste $x \in A$ tale che $x - a \in I$ e $x - b \in J$.
(8) (Artin 10.5.7) Descrivere l'anello ottenuto a partire da $\mathbb{Z}$ e aggiungendo un elemento α che soddisfa entrambe le relazioni $\alpha^3 + \alpha^2 + 1 = 0$ e $\alpha^2 + \alpha = 0$.
(9) (Artin 10.7.2) Determinare gli ideali massimali dei seguenti anelli: (a) $\mathbb{R} \times \mathbb{R}$, (b) $\mathbb{R}[x]/(x^2)$, (c) $\mathbb{R}[x]/(x^2 - 3x + 2)$, (d) $\mathbb{R}[x]/(x^2 + x + 1)$.
(10) (Artin 11.1.6) Calcolare il massimo comun divisore dei seguenti polinomi p, q a coefficienti razionali $p := x^3 - 6x^2 + x + 4$, $q := x^5 - 6x + 1$.
(11) (Artin 11.1.7) Dimostrare che, per ogni campo $\mathbb{F}$, esistono infiniti polinomi irriducibili monici in $\mathbb{F}[x]$.
(12) (Artin 11.4.1) Dimostrare che i polinomi seguenti sono irriducibili in $\mathbb{Q}[x]$:

$$(b)\ x^3 + 6x + 12; \quad (c)\ 8x^3 - 6x + 1; \quad (d)\ x^3 + 6x^2 + 7; \quad (e)\ x^5 - 3x^4 + 3.$$

(13) (Artin 11.4.2) Scomporre il polinomio $x^5 + 5x + 5$ in fattori irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{F}_2[x]$.
(14) (Artin 11.4.3) Scomporre $x^3 + x + 1$ in fattori irriducibili in $\mathbb{F}_p[x]$ per $p = 2, 3, 5$.
(15) (Artin 11.5.3) Scomporre i seguenti interi di Gauss in primi in $\mathbb{Z}[i]$: (a) $1 - 3i$; (b) 10; (c) $6 + 9i$.
(16) (Artin 11.5.6) Sia $p \in \mathbb{Z}$ un primo. Dimostrare che p è un elemento primo di $\mathbb{Z}[\sqrt{3}]$ se e solo se il polinomio $x^2 - 3$ è irriducibile in $\mathbb{F}_p[x]$.
(17) (Artin 11.6.3) Siano d, d' interi distinti privi di quadrati (ossia non divisibili per p^2 per alcun primo p). Dimostrare che $\mathbb{Q}(\sqrt{d})$ e $\mathbb{Q}(\sqrt{d'})$ sono sottocampi distinti di $\mathbb{C}$.

Moduli su un anello.

(1) Esprimere il gruppo abeliano $A := \mathbb{Z}/(12) \times \mathbb{Z}/(15) \times \mathbb{Z}/(18)$ come prodotto diretto di gruppi ciclici $\mathbb{Z}/(d_i)$, dove d_i divide d_j quando $i \leq j$.
Esprimere A anche come prodotto diretto di gruppi del tipo $\mathbb{Z}/(p^k)$ con p primo.

(2) Considerare l'applicazione lineare $L_M : \mathbb{C}^3 \to \mathbb{C}^3$ associata alla seguente matrice complessa

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}.$$

Determinare la forma canonica di Smith della matrice $xI - M$.
Determinare la forma canonica di Jordan di L_M e una base di $\mathbb{C}^3$ di Jordan per L_M.

(3) Sia $T : \mathbb{Q}^3 \to \mathbb{Q}^3$ una applicazione lineare tale che $(T^7 + 2I)(T^2 + 3T + 2I)^2 = 0$. Determinare le possibili forme di Jordan di T e il relativo polinomio caratteristico.

(4) Se $R = \mathbb{C}[x, y]$, sia $I \subseteq R$ l'ideale generato da x e y. Dire se I possieda una base come R-modulo.

(5) Sia R un anello. Descrivere tutti gli omomorfismi di R-moduli $R \to R$.

(6) Un R-modulo si dice *semplice* se gli unici suoi sottomoduli sono quelli banali. Mostrare che se S, S' sono R-moduli semplici, allora un R-omomorfismo $S \to S'$ è un isomorfismo oppure manda ogni elemento in 0.

(7) Sia U il sottogruppo del gruppo abeliano $\mathbb{Z}^3$ generato dagli elementi $(3, 1, 2), (1, 1, 3), (2, 1, 6)$. Esibire una base v_1, v_2, v_3 di $\mathbb{Z}^3$ e interi positivi $d_1|d_2|d_3$ tali che U sia generato da d_1v_1, d_2v_2, d_3v_3.

(8) Dire quanti siano, a meno di isomorfismo, i gruppi abeliani di ordine 400.

(9) Mostrare che se il gruppo abeliano $\mathbb{Q}$ è prodotto diretto di due sottogruppi H, K, allora uno di essi coincide con $\{0\}$.

(10) Dato un anello commutativo con unità, descrivere gli ideali $I \subseteq R$ tali che l'R-modulo R/I sia libero, cioè possieda una base come R-modulo.

(11) Sia R un anello (commutativo con 1) e sia V un R-modulo libero di rango finito. Dimostrare o confutare ciascuna delle seguenti due affermazioni:
   (a) Ogni insieme di generatori contiene una base.
   (b) Ogni insieme linearmente indipendente può essere esteso ad una base.

(12) Sia $\varphi : \mathbb{Z}^k \to \mathbb{Z}^k$ un omomorfismo dato dalla moltiplicazione per la matrice intera A. Dimostrare che limmagine di φ è di indice finito in $\mathbb{Z}^k$ se e solo se A è non singolare e che, in tal caso, l'indice di $\mathrm{Im}(\varphi)$ in $\mathbb{Z}^k$ è pari a $|\det(A)|$.

(13) Sia $p(t)$ un polinomio monico a coefficienti in un campo $\mathbb{F}$. Dimostrare che esiste una matrice $n \times n$ a elementi in $\mathbb{F}$ tale che che abbia polinomio caratteristico $(-1)^n p(t)$.

(14) L'*annullatore* di un R-modulo V è l'insieme $I = \{r \in R \,|\, rv = 0 \text{ per ogni } v \in V\}$. Dimostrare che I è un ideale di R. Determinare l'annullatore dei seguenti $\mathbb{Z}$-moduli: (a) $V = \mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$; (b) $V = \mathbb{Z}$.

Estensioni di campi.

Ex.1 - Determinare il polinomio minimo di $\sqrt{3} + \sqrt{5}$ su ciascuno dei seguenti campi:
(a) $\mathbb{Q}$; (b) $\mathbb{Q}[\sqrt{5}]$; (c) $\mathbb{Q}[\sqrt{10}]$; (d) $\mathbb{Q}[\sqrt{15}]$.

Ex.2 - Sia α una radice complessa del polinomio irriducibile $x^3 - 3x + 4 \in \mathbb{Q}[x]$. Scrivere esplicitamente l'inverso di $\alpha^2 + \alpha + 1$ nella forma $a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{Q}$.

Ex.3 - Sia $\mathbb{F}$ un campo e α un elemento che genera un estensione $\mathbb{F}[\alpha]$ di $\mathbb{F}$ di grado 5. Dimostrare che $\mathbb{F}[\alpha^2] = \mathbb{F}[\alpha]$.

Ex.4 - Dimostrare che $\zeta_5 \notin \mathbb{Q}[\zeta_7]$, dove $\zeta_n = e^{2\pi i/n}$.

Ex.5 - Ponendo $\zeta_n = e^{2\pi i/n}$, determinare il polinomio minimo su $\mathbb{Q}$ di ciascuno dei seguenti elementi: (a) ζ_4; (b) ζ_6; (c) ζ_8; (d) ζ_9; (e) ζ_{10}; (f) ζ_{12}.

Ex.6 - Sia p un numero primo e $q(x) \in \mathbb{F}_p[x]$. Mostrare che se α è una radice di $q(x)$ in un'estensione K di $\mathbb{F}_p$, allora anche α^p annulla $q(x)$.

Ex.7 - Usare l'esercizio precedente per mostrare che, se $q(x) \mid x^p - x - 1$ in $\mathbb{F}_p[x]$, allora $q(x)$ ha grado p. Ovvero $x^p - x - 1$ è irriducibile in $\mathbb{F}_p[x]$.

Ex.8 - Sia p un numero primo e $f(x) \in \mathbb{F}_p[x]$ tale che $f'(x) = 0$. Mostrare che $f(x)$ non è irriducibile.

Ex.9 - I due campi $\mathbb{F}_2[x]/(x^3+x+1)$ e $\mathbb{F}_2[x]/(x^3+x^2+1)$ hanno entrambi otto elementi e sono quindi isomorfi. Costruire tutti gli isomorfismi tra i due campi.

Ex.10 - Quanti sono i polinomi irriducibili monici di grado 3 a coefficienti in $\mathbb{F}_3$ e in $\mathbb{F}_5$?

Ex.11 - Sia K un campo con p^n elementi, $\alpha \in K$ un generatore del gruppo ciclico $K^\times$. Mostrare che il polinomio minimo di α su $\mathbb{F}_p$ ha grado n.

Ex.12 - Sia $\alpha \in \mathbb{C}$ una radice del polinomio $x^3 + x + 1$. Calcolare il polinomio minimo di $\alpha^2 + 1$ su $\mathbb{Q}$.

Ex.13 - Siano $\alpha, \beta \in \mathbb{C}$ radici, rispettivamente, dei polinomi $f(x), g(x) \in \mathbb{Q}[x]$. Poniamo $K = \mathbb{Q}(\alpha), L = \mathbb{Q}(\beta)$. Mostrare che $f(x)$ è irriducibile in $L[x]$ se e solo se $g(x)$ è irriducibile in $K[x]$.

Ex.14 - Sia $q(x) \in K[x]$ un polinomio irriducibile a coefficienti nel campo K di caratteristica 0. Mostrare che $q(x)$ divide $MCD(f(x), f'(x))$, dove $f(x) \in K[x]$, se e solo se $q(x)^2$ divide $f(x)$.

Ex.15 - Dato un poligono regolare P con n lati, dire se sia possibile costruire con riga e compasso un quadrato Q con area uguale all'area di P.

Ex.16 - Dati $p, q \in \mathbb{C}[x]$ non nulli e senza fattori comuni, il *grado* di $f = p/q$ è il massimo dei gradi di p e q. Considerare l'applicazione $\tilde{f} : \mathbb{C} \setminus Z(q) \to \mathbb{C}$ indotta da f, dove $Z(q)$ è l'insieme delle radici di q.
Dimostrare che $\tilde{f}^{-1}(y_0)$ contiene al più d punti e che esiste un sottoinsieme finito $\Delta \subset \mathbb{C}$ tale che $f^{-1}(y_0)$ consiste esattamente di d punti per tutti gli $y_0 \in \mathbb{C} \setminus \Delta$.

Ex.17 - Dimostrare che $f(x) \in \mathbb{C}(x)$ genera $\mathbb{C}(x)$ su $\mathbb{C}$ se e solo se f è della forma $f(x) = (ax+b)/(cx+d)$ con $a, b, c, d \in \mathbb{C}$ e $ad-bc \neq 0$. Determinare il gruppo dei $\mathbb{C}$-automorfismi di $\mathbb{C}(x)$.

Ex.18 - Fattorizzare i polinomi $x^9 - x$ e $x^{27} - x$ in $\mathbb{F}_3[x]$.

Ex.19 - Sia $K = \mathbb{F}_p(t)$ e sia $f(x) = x^p - t \in K[x]$. Dimostrare che f è irriducibile in $K[x]$. Dimostrare che, se f ha una radice α in $L \supset K$, allora α non è una radice semplice.

Ex.20 - Sia K un campo e sia $\overline{K}$ la sua chiusura algebrica. Se K è finito, dimostrare che $\overline{K}$ ha cardinalità infinita numerabile. Se K è infinito, dimostrare che $\overline{K}$ ha la stessa cardinalità di K.