Università di Bologna C.d.L. in Matematica A.A. 2003–04

Scritto di Algebra II (M. Manaresi) – 13.1.04

Giustificare sempre le risposte!

Esercizio 1. Sia $\mathbb{Q}$ il campo dei razionali.

a) Trovare $f \in \mathbb{Q}[x]$ per il quale 1 sia radice doppia e sia $f(0) = 1/2$ e $f(-1) = 1$. E'possibile trovare un tale f irriducibile ?

b) Sia $g \in \mathbb{Q}[x]$ con $\deg(g) < n$; mostrare che se esistono n numeri razionali distinti, $q_1, q_2, \ldots, q_n$, per cui $g(q_1) = g(q_2) = \ldots = g(q_n) = t$ allora g è il polinomio costante t.

c) Mostrare che il polinomio $f = x^4 - 5x^2 + 3$ è irriducibile in $\mathbb{Q}[x]$.

Esercizio 2. Siano, $\mathbb{Z}$ l'anello degli interi, $\mathbb{Q}$ il campo dei razionali e $\mathbb{Z}[i]$ l'anello degli interi di Gauss.

a) È vero che $\mathbb{Q}(i)$ è il campo dei quozienti di $\mathbb{Z}[i]$? Motivare la risposta.

b) Siano $\alpha = 15+45\,i$ e $\beta = 7-21\,i$ due elementi di $\mathbb{Z}[i]$; determinare un generatore γ dell'ideale (α, β) di $\mathbb{Z}[i]$ da essi generato.

c) Mostrare che non esiste alcun morfismo di anelli $\psi : \mathbb{Z}[i] \to \mathbb{Z}$.

d) È vero che gli unici morfismi di anelli da $\mathbb{Z}[i]$ a $\mathbb{Z}[i]$ stesso sono, l'identità e il coniugio ?

Esercizio 3. Siano $\mathbb{Q}$ ed $\mathbb{R}$ i campi dei razionali e dei reali e sia u il numero complesso $\sqrt{i} - i$ dove con $\sqrt{i}$ si indica quella tra le due radici quadrate di i che ha parte reale positiva.

a) Scrivere u nella forma canonica $a + bi$ con $a, b \in \mathbb{R}$.

b) Trovare il polinomio minimo p_u di u in $\mathbb{Q}[x]$.

c) Decomporre p_u nel prodotto di irriducibili in $\mathbb{R}[x]$.

d) Mostrare che $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(u)$ e che $\mathbb{Q}(i) \subseteq \mathbb{Q}(u)$. Risulta $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(u)$?

e) Qual è il grado di $\mathbb{Q}(u)$ su $\mathbb{Q}(i)$?

Esercizio 4. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$ ed f sia il polinomio $x^2 + x + [1]_5$. Poniamo poi $F = \mathbb{Z}_5[x]/(f)$ ed $\epsilon = [x]_{(f)}$ e identifichiamo ogni $a \in \mathbb{Z}_5$ con la classe $[a]_{(f)}$.

a) Mostrare che F è un campo e trovarne la cardinalità e la caratteristica.

b) Trovare $a_0, b_0, a_1, b_1 \in \mathbb{Z}_5$ tali che $\epsilon^2 = a_0 + b_0\epsilon$ e $([2]_5 + \epsilon)^{-1} = a_1 + b_1\epsilon$.

c) Il polinomio $y^2 + [2]_5$ di $F[y]$ ha radici in F ?

d) Trovare il campo di spezzamento K del polinomio $g = (x^2 + x + [1]_5)(x^2 + [2]_5) \in \mathbb{Z}_5[x]$ e calcolare $[K : \mathbb{Z}_5]$.

Università di Bologna **C.d.L. in Matematica** **A.A. 2003–04**

Scritto di Algebra II (M. Manaresi) – 10.2.04

Giustificare sempre le risposte!

Esercizio 1. Sia $\mathbb{Q}[x]$ l'anello dei polinomi a coefficienti razionali, $\mathbb{C}$ il campo complesso e sia $f = x^4 - x^3 + 2x^2 - x + 1$.

a) Verificare che il numero complesso i è radice di f.
b) Dalla risposta a) segue che il polinomio $x^2 + 1$ divide f in $\mathbb{Q}[x]$?
c) Decomporre f nel prodotto di irriducibili in $\mathbb{Q}[x]$ e in $\mathbb{C}[x]$.
d) Trovare $g \in \mathbb{Q}[x]$ tale che $g(1) = 0$, $\deg(g) < 4$ e l'ideale $(f) + (g) \neq (1)$ in $\mathbb{Q}[x]$.

Esercizio 2. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss, $r = 357$ e $s = 3 + 5i$ due suoi elementi ed I sia l'ideale di $\mathbb{Z}[i]$ generato da $\{r, s\}$.

a) Trovare un massimo comun divisore di r e s.
b) Mostrare che l'ideale I è primo.
c) Esiste in $\mathbb{Z}[i]$ un ideale $J \neq I$ tale che $(s) \subset J \subset \mathbb{Z}[i]$? (inclusioni proprie)
d) Trovare una soluzione (in $\mathbb{Z}[i]$) della congruenza $(3 + i)x \equiv 5 \pmod 7$.

Esercizio 3. Siano $\mathbb{Q}$ ed $\mathbb{R}$ i campi dei razionali e dei reali e sia u il numero complesso $\sqrt{5} - i$.

a) Si dimostri che $\sqrt{5}$ appartiene a $\mathbb{Q}(u)$.
b) Si dimostri che u é algebrico su $\mathbb{Q}$ e si calcoli il polinomio minimo p_u di u in $\mathbb{Q}[x]$.
c) Si stabilisca se $\mathbb{Q}(u)$ é il campo di spezzamento del polinomio p_u su $\mathbb{Q}$.

Esercizio 4. Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_3$ e siano $f = x^5 + x^4 - x^3 - x^2 - x + [1]_3$, $g = x^2 + x + [2]_3$ e $h = x^2 - x + [2]_3$ tre suoi elementi.

a) Trovare le radici di f in $\mathbb{Z}_3$ con le relative molteplicità.
b) Qual è la caratteristica dell'anello quoziente $\mathbb{Z}_3[x]/(f)$?
c) Trovare un generatore dell'ideale $(f) \cap (g)$ di $\mathbb{Z}_3[x]$.
d) Trovare i campi di spezzamento L e K di f e di g su $\mathbb{Z}_3$ e calcolare $[L : \mathbb{Z}_3]$ e $[K : \mathbb{Z}_3]$.
e) È vero che gli anelli $\mathbb{Z}_3[x]/(g)$ e $\mathbb{Z}_3[x]/(h)$ sono isomorfi ? Se sì esplicitare l'isomorfimo.

Scritto di Algebra II (M. Manaresi) – 10.1.05

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi, con esclusione del punto 2-d.

Esercizio 1. Sia $\mathbb{Z}$ il gruppo additivo degli interi e $\mathbb{Z}_{18}$ il gruppo delle classi di resti modulo 18.

a) Trovare due sottogruppi propri, $S \subset \mathbb{Z}$ e $T \subset \mathbb{Z}_{18}$, tali che i gruppi quoziente $\mathbb{Z}/S$ e $\mathbb{Z}_{18}/T$ siano isomorfi.
b) È vero che esistono esattamente 6 omomorfismi di gruppi suriettivi da $\mathbb{Z}$ a $\mathbb{Z}_{18}$?
c) Trovare tutti gli omomorfismi di gruppi $\phi : \mathbb{Z} \to \mathbb{Z}_{18}$ tali che $\phi(50) = [0]_{18}$.
d) È vero che per ogni omomorfismo di gruppi $\psi : \mathbb{Z} \to \mathbb{Z}_{18}$ se $|\operatorname{Im}(\psi)| = 6$ allora $\ker \psi = 6\mathbb{Z}$?

Esercizio 2. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$, siano $f = x^4 + [2]_5 x^3 + [3]_5 x^2 + [4]x + [2]_5$ e $g = x^4 + x^3 + [3]_5 x^2 + [2]_5 x + [2]_5$ due suoi elementi e sia $A := \mathbb{Z}_5[x]/(f)$ l'anello quoziente di $\mathbb{Z}_5[x]$ rispetto all'ideale (f).

a) Stabilire se il laterale $(f) + x^5 + [3]_5 x + [2]_5$ contiene polinomi di grado due.
b) Stabilire se i laterali $(f) + x$ e $(f) + g$ sono elementi invertibili dell'anello A e, in caso affermativo, determinare i loro inversi.
c) Stabilire se nell'anello quoziente A esistono elementi nilpotenti.
d) Stabilire se gli anelli quoziente $A := \mathbb{Z}_5[x]/(f)$ e $B := \mathbb{Z}_5[x]/(g)$ sono isomorfi.
e) Determinare il campo di spezzamento K di f su $\mathbb{Z}_5$ e stabilire se su K anche g si spezza in fattori lineari.

Esercizio 3. Sia $\mathbb{Q}$ il campo dei razionali e consideriamo le seguenti 4 sue estensioni; $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}\,i)$, $\mathbb{Q}(\sqrt{2} + \sqrt{2}\,i)$ e $\mathbb{Q}(\sqrt{2}, \sqrt{2}\,i)$.

a) Mostrare che i campi $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{2}\,i)$ non sono isomorfi.
b) Provare che $\sqrt{2} - \sqrt{2}\,i \in \mathbb{Q}(\sqrt{2} + \sqrt{2}\,i)$. (Sugg.: calcolare l'inverso di $\sqrt{2} + \sqrt{2}\,i$)
c) È vero che per nessun campo F si ha $\mathbb{Q}(\sqrt{2}) \subset F \subset \mathbb{Q}(\sqrt{2}, \sqrt{2}\,i)$?
d) Mostrare, per esempio usando b), che $\mathbb{Q}(\sqrt{2} + \sqrt{2}\,i) = \mathbb{Q}(\sqrt{2}, \sqrt{2}\,i)$.

Esercizio 4. Siano, $\mathbb{Z}[i]$ l'anello degli interi di Gauss, $\alpha = 17 - 6i$ e $\beta = 7 - 17i$ due suoi elementi e J l'ideale di $\mathbb{Z}[i]$ generato da $\{\alpha, \beta\}$.

a) Calcolare un massimo comun divisore di α e β.
b) L'anello quoziente $\mathbb{Z}[i]/J$ è un campo ?
c) Decomporre α nel prodotto di irriducibili di $\mathbb{Z}[i]$.
d) Stabilire se esistono, eventualmente senza determinarli esplicitamente, $\lambda_1, \lambda_2 \in \mathbb{Z}[i]$ tali che $\alpha\lambda_1 + \beta\lambda_2 = 26$.

Informatico-Computazionale A.A. 2004–05

Prova scritta di Algebra II (M. Manaresi) – 15.6.05

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi con l'esclusione del punto **2-d**.

Esercizio 1. Siano $\mathbb{Z}_2$, $\mathbb{Z}_{16}$ e $\mathbb{Z}_{32}$ i gruppi delle classi di resti modulo, 2, 16 e 32.

a) Mostrare che $\mathbb{Z}_{32}$ non è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_{16}$.
b) Trovare un sottogruppo proprio H di $\mathbb{Z}_{32}$ ed un sottogruppo proprio K di $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ tali che i gruppi quoziente $\mathbb{Z}_{32}/H$ e $\mathbb{Z}_2 \times \mathbb{Z}_{16}/K$ siano isomorfi.
c) Trovare un morfismo $\psi : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ tale che $\mathrm{Im}(\psi) = \ker \psi$.
d) È vero che se G è un gruppo finito ed esiste un morfismo $f : G \to G$ tale che $\mathrm{Im}(f) = \ker f$ allora l'ordine di G è il quadrato di un intero ?

Esercizio 2. Sia $\mathbb{Q}$ il campo dei razionali, A l'anello $\mathbb{Q}[x] \times \mathbb{Q}[x]$ e J ed H siano gli ideali di A generati, rispettivamente, da $(x, x^2 - 2)$ e da $(5, x^2 - 2)$.

a) Mostrare che l'ideale J è contenuto propriamente nell'ideale H.
b) Verificare che H è un ideale massimale.
c) Si determini un ideale primo I dell'anello A che non sia contenuto in H e si studi l'anello quoziente A/I.
d) È vero che l'anello quoziente A/H è isomorfo a $\mathbb{Q}(\sqrt{2})$?

Esercizio 3. Sia $\mathbb{Q}$ il campo dei razionali e $\mathbb{Q}(u)$ la sua estensione ottenuta con l'aggiunta del numero reale $u = -2 + \sqrt[3]{6}$.

a) Trovare il polinomio minimo, p_u, di u in $\mathbb{Q}[x]$.
b) Qual è il grado di $\mathbb{Q}(u^{-1})$ su $\mathbb{Q}$?
c) Scrivere u^{-1} nella forma canonica $q_0 + q_1 u + q_2 u^2 + \ldots + q_{n-1} u^{n-1}$ con i $q_k \in \mathbb{Q}$ e $n = \deg(p_u)$.
d) Mostrare che se $q \in \mathbb{Q}$ e $\sqrt{q} \in \mathbb{Q}(u)$ allora $\sqrt{q} \in \mathbb{Q}$ (Suggerimento: una possibile via è quella di studiare $[\mathbb{Q}(\sqrt{q}) : \mathbb{Q}]$ ...)

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss ed $u = 5 + 5i$ e $v = 4 + 2i$ siano 2 suoi elementi.

a) Trovare un massimo comun divisore d di u e v.
b) Mostrare che l'anello quoziente $\mathbb{Z}[i]/(d)$ non è un dominio di integrità.
c) Verificare che $\mathbb{Z}[i]/(d)$ ha caratteristica di 10.

Università di Bologna C.d.L. in Matematica C.d.L. in Matematica Informatico-Computazionale A.A. 2004–05

Prova scritta di Algebra II (M. Manaresi) – 7.7.05

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi con l'esclusione del punto **2-d**.

Esercizio 1. Sia $\mathbb{Z}_3 \times \mathbb{Z}$ il gruppo prodotto diretto del gruppo delle classi di resti modulo 3 e di quello degli interi e $f : \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}$ sia un morfismo di gruppi.

a) Definire f in modo che risulti iniettivo.
b) f può essere suriettivo ?
c) Mostrare che se in $\mathrm{Im}(f)$ vi è un elemento di periodo 3 allora $\mathrm{Im}(f)$ è un insieme finito.
d) Esiste f tale che $\ker f = 6\mathbb{Z}$?

Esercizio 2. Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_3$ e J_1 e J_2 siano gli ideali di $\mathbb{Z}_3[x]$ generati, rispettivamente, dai polinomi $x^3 + [2]_3 x + [2]_3$ e $[2]_3 x^3 + [2]_3 x^2 + [1]_3$.

a) Mostrare che l'anello quoziente $\mathbb{Z}_3[x]/(J_1)$ è un campo.
b) È vero che gli anelli $\mathbb{Z}_3[x]/(J_1)$ e $\mathbb{Z}_3[x]/(J_2)$ sono isomorfi ?
c) Trovare la forma ridotta dell'elemento $J_1 + x^4 + [2]_3$ di $\mathbb{Z}_3[x]/(J_1)$.
d) Elencare i sottocampi di $\mathbb{Z}_3[x]/(J_1)$.

Esercizio 3. Sia $\mathbb{R}$ il campo dei reali, $\mathbb{Q}[x]$ l'anello dei polinomi a coefficienti nel campo dei razionali ed $f = x^5 - x^4 - 4x^3 + 4x^2 + 2x - 2$ sia un elemento di $\mathbb{Q}[x]$.

a) Verificare che f ha una radice in $\mathbb{Q}$.
b) Decomporre f nel prodotto di irriducibili di $\mathbb{Q}[x]$.
c) Mostrare che f si decompone in $\mathbb{R}[x]$ nel prodotto di fattori lineari.
d) È vero che $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ è un campo di spezzamento su $\mathbb{Q}$ di f ? (Suggerimento: mostrare che $\sqrt{2} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$ e che $1/\sqrt{2+\sqrt{2}} = \ldots.$)

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss e $w = 70$ sia un suo elemento.

a) Decomporre w nel prodotto di irriducibili di $\mathbb{Z}[i]$.
b) Detto J l'ideale di $\mathbb{Z}[i]$ generato da w, elencare gli ideali massimali di $\mathbb{Z}[i]$ che contengono J.
c) Trovare, se esiste, nell'anello quoziente $\mathbb{Z}[i]/J$ un elemento $J + u$ per il quale risulti $(J+3)(J+u) = J+1$.

Università di Bologna C.d.L. in Matematica C.d.L. in Matematica Informatico-Computazionale A.A. 2004–05

Prova scritta di Algebra II (M. Manaresi) – 14.9.05

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\mathbb{Z}$ il gruppo degli interi, S_6 il gruppo delle permutazioni sull'insieme $\{1,2,3,4,5,6\}$ e $\sigma = (1\,5\,4\,6)\circ(1\,2\,3\,5\,4)$, $\tau = (1\,2)\circ(3\,5\,6)$ due elementi di S_6.

a) Mostrare che i sottogruppi $\langle\sigma\rangle$ e $\langle\tau\rangle$ di S_6 sono isomorfi.

b) σ e τ sono coniugati in S_6 ?

c) È vero che per tutti i morfismi $\phi : \mathbb{Z} \to S_6$ risulta $\langle\sigma\rangle \cap \langle\tau\rangle \subseteq \mathrm{Im}(\phi)$?

Esercizio 2. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$ e siano $f = x^5 - x^4 - x^3 + [2]_5 x + [3]_5$ e $g = x^4 + [3]_5 x^2 + [2]_5 x + [3]_5$ due suoi elementi.

a) Determinare un polinomio d di $\mathbb{Z}_5[x]$ tale che risulti: $(d) = (f,g)$.

b) Trovare un ideale massimale J di $\mathbb{Z}_5[x]$ tale che $(d) \subseteq J$

c) Trovare, se esiste, l'inverso di $(d) + x + [2]_5$ nell'anello quoziente $\mathbb{Z}_5[x]/(d)$.

d) Se $\phi : \mathbb{Z}_5[x] \to \mathbb{Z}_5[x]$ è un morfismo di anelli, mostrare che se $\mathrm{Im}(\phi)$ è un insieme infinito allora ϕ è iniettivo. (Possibile via: studiare $\mathbb{Z}_5[x]/\ker\phi$ ...).

Esercizio 3. Siano $\mathbb{Q}$ ed $\mathbb{R}$ i campi dei razionali e dei reali ed u sia il numero reale $\sqrt{3+\sqrt{11}}$.

a) Trovare il polinomio minimo p_u di u in $\mathbb{Q}[x]$.

b) Mostrare che $\mathbb{Q}(\sqrt{11}) \subseteq \mathbb{Q}(u)$.

c) Decomporre p_u nel prodotto di irriducibili di $\mathbb{R}[x]$.

d) Trovare il campo di spezzamento K di p_u su $\mathbb{Q}$, stabilendo in particolare se $K = \mathbb{Q}(u)$. (Possibile via: ricordare che $\mathbb{Q}(u) \subseteq \mathbb{R}$ ...).

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss e $\alpha = 2+4i$, $\beta = 4-6i$, $\gamma = 73$ siano tre suoi elementi.

a) Decomporre γ nel prodotto di irriducibili di $\mathbb{Z}[i]$.

b) Se J è l'ideale di $\mathbb{Z}[i]$ generato da $\{\alpha,\beta\}$, trovare $\omega \in \mathbb{Z}[i]$ tale che $J = (\omega)$.

c) Mostrare che l'anello quoziente $\mathbb{Z}[i]/J$ ha 4 soli elementi e stabilire se è un campo.

d) Trovare la caratteristica di $\mathbb{Z}[i]/J$.

Università di Bologna C.d.L. in Matematica C.d.L. in Matematica Informatico-Computazionale A.A. 2004–05

Prova scritta di Algebra II (M. Manaresi) – 27.9.05

Giustificare sempre le risposte!

Gli studenti di ALGEBRA COMPUTAZIONALE I debbono svolgere i primi due esercizi.

Esercizio 1. Siano, $\mathbb{Z}$, $\mathbb{Z}_{14}$ e $\mathbb{Z}_{24}$ i gruppi, rispettivamente, degli interi e delle classi di resti modulo 14 e modulo 24.

a) Trovare due sottogruppi propri, $S_1 \subseteq \mathbb{Z}_{14}$ e $S_2 \subseteq \mathbb{Z}_{24}$ tali che i gruppi quoziente $\mathbb{Z}_{14}/S_1$ e $\mathbb{Z}_{24}/S_2$ siano isomorfi.
b) È vero che non esiste alcun epimorfismo da $\mathbb{Z}_{24}$ a $\mathbb{Z}_{14}$?
c) Mostrare che se $\phi : \mathbb{Z} \to \mathbb{Z}_{14}$ è un morfismo e $\phi(25) = [0]_{14}$ allora ϕ è il morfismo nullo.

Esercizio 2. Sia A il sottoanello del campo $\mathbb{Q}$ dei razionali costituito da tutte le frazioni che in forma ridotta hanno il denominatore primo con 7 e sia J l'ideale di A generato da 7.

a) È vero che 4/3 e 1/8 sono invertibili in A ?
b) Mostrare che A, come anello, non è isomorfo all'anello $\mathbb{Z}$ degli interi.
c) Provare che l'ideale J è massimale. (Possibile via: se $r/s \notin J$ allora 7 non divide r e quindi r/s è un elemento ...).
d) Verificare che esiste $m \in \mathbb{Z}$ per cui $J + 2/5 = J + m$.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei razionali e dei complessi e poi siano, $v \in \mathbb{C}$ diverso da 2 e $z = (v+1)/(v-2)$.

a) Mostrare che $\mathbb{Q}(v) = \mathbb{Q}(z)$.
b) Verificare che; v è algebrico $\iff$ z è algebrico.
c) Se v e z sono algebrici e p_v e p_z sono i loro polinomi minimi in $\mathbb{Q}[x]$, è vero che $\deg(p_v) = \deg(p_z)$?
d) Trovare p_v se $p_z = x^2 + x - 1$.

Esercizio 4. Siano, $\mathbb{Z}[i]$ l'anello degli interi di Gauss, $\mathbb{N}$ l'insieme dei naturali e, per ogni $t \in \mathbb{N}$, sia ω_t l'elemento di $\mathbb{Z}[i]$ così definito; $\omega_t = t - 2 + (2t+1)\,i$.

a) Trovare un generatore dell'ideale $(\omega_2) \cap (\omega_3)$ di $\mathbb{Z}[i]$.
b) Verificare che $1 + 2i$ divide ω_t per ogni $t \in \mathbb{N}$.
c) Nell'anello quoziente $\mathbb{Z}[i]/(\omega_2)$ trovare, se esiste, l'inverso di $(\omega_2) + 1 + i$.

Informatico-Computazionale A.A. 2005–06

Esercitazione scritta di Algebra II (M. Manaresi) – 17.12.05

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\psi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ l'applicazione definita da: $\psi(x,y) = (0, 2x+5y)$.

a) Mostrare che ψ è un omomorfismo di gruppi nè iniettivo nè suriettivo.
b) Determinare $ker(\psi)$ e dimostrare che $Im(\psi) = \{0\}\times\mathbb{Z}$
c) Ci sono elementi di ordine 10 nel gruppo quoziente $\mathbb{Z}\times\mathbb{Z}/ker(\psi)$?
d) Stabilire se il gruppo quoziente $\mathbb{Z}\times\mathbb{Z}/ker(\psi)$ è ciclico.

Esercizio 2. Sia $\mathbb{Z}_7[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_7$, siano $f = x^3+x^2+[5]_7x+[5]_7$ e $g = x^3+[2]_7x^2+[5]_7x+[3]_7$ due suoi elementi, sia $I = (f,g)$ e sia $A := \mathbb{Z}_7[x]/I$ l'anello quoziente dell'anello $\mathbb{Z}_7[x]$ rispetto all'ideale I.

a) Stabilire se nell'anello A vi sono zero-divisori.
b) Stabilire se l'elemento $I+x$ è invertibile in A e in caso positivo trovarne l'inverso.
c) Stabilire se le applicazioni $\sigma : A := \mathbb{Z}_7[x]/I \to B := \mathbb{Z}_7[x]/(x^2+2)$, data da $\sigma([h]_I) = [h]_{(x^2+2)}$, e $\tau : C := \mathbb{Z}_7[x]/(g) \to A := \mathbb{Z}_7[x]/I$, data da $\tau([h]_{(g)}) = [h]_I$, sono ben definite e sono omomorfismi di anelli. In caso affermativo determinarne nucleo e immagine.

Esercizio 3. Sia $u \in \mathbb{C}$ un elemento algebrico su $\mathbb{Q}$, che è radice del polinomio $f = x^5+2x^3+x^2+x+1 \in \mathbb{Q}[x]$, ma non è radice del polinomio $g = x^4+2x^2+1 \in \mathbb{Q}[x]$.

a) Trovare il polinomio minimo p_u di u su $\mathbb{Q}$.

b) u è univocamente determinato?

c) Se suppongo che $u \in \mathbb{R}$, u è univocamente determinato?
[Possibile via: studiare la derivata del polinomio p_u per stabilire quante sono le radici reali di tale polinomio.]

d) Sia $u \in \mathbb{R}$ e siano $\mathbb{Q}(u)$ l' estensione di $\mathbb{Q}$ ottenuta con l'aggiunta del numero reale u e L il campo di spezzamento del polinomio p_u su $\mathbb{Q}$. Si stabilisca quali relazioni di inclusione sussistono fra i campi $\mathbb{Q}, \mathbb{Q}(u), L$ e si calcolino i gradi di tutte le estensioni.

d) Sia K il campo di spezzamento del polinomio $f = x^5+[2]_5x^3+x^2+x+[1]_5$ su $\mathbb{Q}$. Si stabilisca se $K = L$.

Esercizio 4. Stabilire se esistono gli omomorfismi di anelli di cui ai punti seguenti e in caso positivo scrivere gli omomorfismi.

a) Esiste un omomorfismo di anelli dal campo $\mathbb{Q}(x)$ nel campo $\mathbb{C}(x)$?
b) Esiste un omomorfismo di anelli dal campo $\mathbb{Z}_{(13)}$ nel campo $\mathbb{Q}(x)$?
c) Esiste un omomorfismo di anelli dal campo $\mathbb{Z}_{(13)}$ nell'anello quoziente $\mathbb{Z}[i]/(23+11i, 5+i)$, dove $\mathbb{Z}[i]$ è l'anello degli interi di Gauss.

Università di Bologna **C.d.L. in Matematica** **C.d.L. in Matematica Informatico-Computazionale** **A.A. 2005–06**

Prova scritta di Algebra II (M. Manaresi) – 10.1.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Siano $\mathbb{Z}$ e $\mathbb{Z}_{15}$ i gruppi additivi degli interi e delle classi di resto modulo 15 rispettivamente e sia $\mathbb{Z} \times \mathbb{Z}_{15}$ il gruppo prodotto diretto dei gruppi $\mathbb{Z}$ e $\mathbb{Z}_{15}$.

a) Elencare gli omomorfismi di gruppi suriettivi da $\mathbb{Z}$ a $\mathbb{Z}_{15}$.
b) Trovare un omomorfismo di gruppi f_1 da $\mathbb{Z}$ a $\mathbb{Z}_{15}$ tale che $Im(f_1)$ abbia 3 elementi.
c) Esiste un omomorfismo di gruppi f_2 da $\mathbb{Z}$ a $\mathbb{Z}_{15}$ tale che $Ker(f_2)$ sia il sottogruppo $< 30 >$ di $\mathbb{Z}$?
d) Esistono omomorfismi di gruppi suriettivi da $\mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}_{15}$?

Esercizio 2. Sia $\mathbb{Z} \times \mathbb{Q}$ l'anello prodotto diretto dell'anello degli interi e del campo dei razionali e sia I un suo ideale.

a) Determinare un ideale I tale che l'anello quoziente $(\mathbb{Z} \times \mathbb{Q})/I$ abbia tre elementi.
b) E' vero che se I è tale che $(\mathbb{Z} \times \mathbb{Q})/I$ ha 37 elementi, allora $(\mathbb{Z} \times \mathbb{Q})/I$ è un campo?
c) Esistono in $\mathbb{Z} \times \mathbb{Q}$ ideali I che sono primi ma non massimali?
d) Provare che in $\mathbb{Z} \times \mathbb{Q}$ ogni ideale I è principale.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei razionali e dei complessi rispettivamente, sia $u \in \mathbb{C}$ un numero complesso radice del polinomio $x^3 - x + 1 \in \mathbb{Q}[x]$ e sia $v = u^2$.

a) Provare che v è radice del polinomio a coefficienti razionali $x^3 - 2x^2 + x - 1$.
b) Stabilire se $\mathbb{Q}(u) = \mathbb{Q}(v)$.
c) Stabilire se esiste $z \in \mathbb{Q}(u) - \mathbb{Q}$ tale che $z^2 \in \mathbb{Q}$.
d) Sia $w \in \mathbb{C}$ tale che $[\mathbb{Q}(w) : \mathbb{Q}] = 3$. Determinare i possibili valori di $[\mathbb{Q}(u, w) : \mathbb{Q}]$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani.

a) Decomporre 1221 in fattori irriducibili di $\mathbb{Z}[i]$.
b) Trovare un massimo comun divisore d di 1221 e $5 + 7i$.
c) Stabilire se l'anello $\mathbb{Z}[i]/(d)$ è un campo e calcolarne la caratteristica.
d) Stabilire se gli anelli $\mathbb{Z}[i]$ e $\mathbb{Z}[x]$ sono isomorfi e in caso affermativo scrivere l'isomorfismo tra essi.

Università di Bologna C.d.L. in Matematica C.d.L. in Matematica
Informatico-Computazionale A.A. 2005–06

Prova scritta di Algebra II (M. Manaresi) – 31.1.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi ad eccezione del quesito **2. e)**.

Esercizio 1. Sia $S_3 \times \mathbb{Z}_6$ il gruppo prodotto diretto del gruppo delle permutazioni sull'insieme $\{1,2,3\}$ e del gruppo $\mathbb{Z}_6$. Sia $\alpha \in S_3$, $\alpha = (2\,3)$ e sia 1_{S_3} la permutazione identica di S_3.

a) Trovare in $S_3 \times \mathbb{Z}_6$ la classe di coniugio di $(\alpha, [0]_6)$.
b) È vero che il sottogruppo di $S_3 \times \mathbb{Z}_6$ generato da $\{(\alpha, [0]_6), (1_{S_3}, [1]_6)$ è normale ?
c) Elencare i morfismi $\phi : \mathbb{Z} \to S_3 \times \mathbb{Z}_6$ tali che $|\operatorname{Im}(\phi)| = 2$.
d) Esistono omomorfismi di gruppi suriettivi da $\mathbb{Z}$ a $S_3 \times \mathbb{Z}_6$?

Esercizio 2. Sia $K := \mathbb{Z}_3[x]/(2x^2 + x + 1)$, sia $\epsilon = [x]_{(2x^2+x+1)}$.

a) Provare che l'anello K é un campo.
b) Determinare la caratteristica e il numero degli elementi di K.
c) Trovare la forma normale di ϵ^3.
d) Determinare l'inverso di $1 + \epsilon$ in K.
e) Stabilire se in $K[y]$ il polinomio $y^3 + \epsilon$ si decompone in fattori lineari e in caso di risposta negativa si determini il campo di spezzamento di $y^3 + \epsilon$ su K.

Esercizio 3. Siano $\mathbb{Q}$ $\mathbb{R}$ e $\mathbb{C}$ i campi dei razionali, dei reali e dei complessi rispettivamente, sia $u = cos(4\pi/5) + isen(4\pi/5)$ e $v = u + 1$.

a) Tracciare la posizione di u e v nel piano complesso.

b) Determinare i polinomi minimi p_u e p_v su $\mathbb{Q}$.

c) Stabilire se $\mathbb{Q}(u)$ é il campo si spezzamento del polinomio p_u su $\mathbb{Q}$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani, siano I e J due suoi ideali e $\phi : \mathbb{Z}[i]/I \to \mathbb{Z}[i]/J$ un omomorfismo di anelli.

a) L'omomorfismo ϕ è necessariamente suriettivo?
b) Se $\mathbb{Z}[i]/I$ è un dominio d'integrità, anche Z[i]/J lo è?
c) Se $I = (203)$, elencare tutti i possibili J per i quali ϕ è ben definito.
d) Se $J = (9 + 5i)$, trovare tutti i possibili I per i quali ϕ è ben definito.

Informatico-Computazionale A.A. 2005–06

Prova scritta di Algebra II (M. Manaresi) – 21.4.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Siano $\mathbb{Z}_{12}$ e S_4 i gruppi delle classi di resto modulo 12 e delle permutazioni su 4 lettere rispettivamente.

a) Stabilire se tra gli omomorfismi di gruppi da $\mathbb{Z}_{12}$ a S_4 ve ne sono di suriettivi.

b) Stabilire se tra gli omomorfismi di gruppi da $\mathbb{Z}_{12}$ a S_4 ve ne sono di iniettivi.

c) Trovare un omomorfismo di gruppi f_1 da da $\mathbb{Z}_{12}$ a S_4 tale che $Im(f_1)$ abbia 3 elementi.

d) Esiste un omomorfismo di gruppi $f_2 : \mathbb{Z}_{12} \to S_4$ tale che $Ker(f_2)$ sia il sottogruppo $< [3]_{12} >$ di $\mathbb{Z}_{12}$?

Esercizio 2. Si consideri l'anello quoziente $A := \mathbb{Q}[x]/(x^2 - 5x + 6)$ e per ogni $f(x) \in \mathbb{Q}[x]$ si denoti con $[f(x)] := [f(x)]_{(x^2-5x+6)}$ il corrispondente elemento di A. Sia $\pi : \mathbb{Q}[x] \to A$ la proiezione canonica sul quoziente.

a) Stabilire se nell'anello A vi sono zero-divisori non nulli.

b) Trovare un elemento $\alpha \in A$ tale che $[x+2]\alpha = [x+7]$

c) Sia $I := ([x-1])$ l'ideale di $\mathbb{Q}[x]/(x^2 - 5x + 6)$ generato dall'elemento $[x-1]$. Si trovi un ideale proprio $J \subset \mathbb{Q}[x]$ tale che $I \neq J$, ma $\pi(I) = \pi(J)$

d) Si determini un ideale massimale di A.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{R}$ i campi dei razionali e dei reali rispettivamente, sia $u \in \mathbb{R}$ un numero reale radice del polinomio $x^3 - 2 \in \mathbb{Q}[x]$.

a) Si determini il campo di spezzamento L del polinomio minimo p_u di u su $\mathbb{Q}$ e si stabilisca se $L = \mathbb{Q}(u)$.

b) Si consideri il sottoinsieme $U := \{a + bu/a, b \in \mathbb{Q}\}$ di $\mathbb{Q}(u)$. Si stabilisca se $u^2 \in \mathbb{Q}(u)$ e se U é un sottocampo di $\mathbb{Q}(u)$.

c) Si determini la forma normale di $(u^3 + u)u^2 + 2u - (u + 1)$ in $\mathbb{Q}(u)$.

b) Si determini l'inverso moltiplicativo di u^2-1 e la forma normale di $(u+1)/(u^2-1)$ in $\mathbb{Q}(u)$.

Esercizio 4. Sia K un campo e sia $m(x) \in K[x]$ un polinomio a coefficienti in K. Per quali dei seguenti polinomi $m(x)$ e dei seguenti campi K esiste un'estensione $K(u)$ di K tale che u abbia $m(x)$ come polinomio minimo?

a) $m(x) = x^2 + 1$, $K = \mathbb{Z}_3$;

b) $m(x) = x^2 + 1$, $K = \mathbb{Z}_5$;

c) $m(x) = x^7 - 3x^6 + 4x^3 - 1$, $K = \mathbb{R}$;

d) $m(x) = x^2 - 3$, $K = \mathbb{Z}[i]/(5 - i, 13(4 + i))$.

Università di Bologna C.d.L. in Matematica C.d.L. in Matematica Informatico-Computazionale A.A. 2005–06

Prova scritta di Algebra II (**M. Manaresi**) – **6.6.06**

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\mathbb{Z}_{15}^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{15}$ delle classi di resto modulo 15 e sia $\mathbb{Z}_4$ il gruppo additivo delle classi di resto modulo 4.

a) Stabilire quanti sono gli omomorfismi di gruppi da $\mathbb{Z}_4$ a $\mathbb{Z}_{15}^*$.

b) Stabilire se esiste un omomorfismo di gruppi da $\mathbb{Z}_4$ a $\mathbb{Z}_{15}^*$ il cui nucleo sia il sottogruppo $< [2]_4 >$ di $\mathbb{Z}_4$.

c) Stabilire se esistono omomorfismi di gruppi iniettivi da $\mathbb{Z}_4$ a $\mathbb{Z}_{15}^*$.

d) Stabilire se esistono omomorfismi di gruppi suriettivi da $\mathbb{Z}_4$ a $\mathbb{Z}_{15}^*$.

Esercizio 2. Siano A_1 e A_2 due anelli non nulli e sia $f : A_1 \to A_2$ un omomorfismo di anelli.

a) Se f é iniettivo e l'anello A_1 é un campo, anche l'anello A_2 é necessariamente un campo?

b) Mostrare che se f é iniettivo e l'anello A_2 é un campo, l'anello A_1 non é necessariamente un campo.

c) Mostrare che se f é suriettivo e l'anello A_2 é un campo, l'anello A_1 non é necessariamente un campo.

d) Sia $A_1 = \mathbb{Q}[x]$, $A_2 = \mathbb{Q}[x]/(x^2 - 9)$ e f la proiezione canonica sul quoziente. E' vero che ogni ideale proprio dell'anello A_1 é mandato da f in un ideale proprio dell'anello A_2?

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei razionali e dei complessi rispettivamente, sia $u = \sqrt[3]{-5} \in \mathbb{C}$, $\sigma_u : \mathbb{Q}[x] \to \mathbb{C}$ il morfismo sostituzione.

a) Si determini il polinomio minimo p_u di u su $\mathbb{Q}$.

b) Si stabilisca se $u \in \mathbb{Q}(\sqrt{-5})$.

c) Si stabilisca se $\mathbb{Q}(\sqrt{-5}) \subset \mathbb{Q}(u)$.

d) Per quali $a, b, c \in \mathbb{Q}$ risulta $ax^3 + bx^2 + c \in Ker(\sigma_u)$.

e) E' vero che gli elementi di $Im(\sigma_u)$ sono tuttidel tipo: $a + bu$ con $a, b \in \mathbb{Q}$?

Esercizio 4. Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a cefficienti nel campo $\mathbb{Z}_3$, sia $f = x^4 + x^3 + x^2 + [2]_3 \in \mathbb{Z}_3[x]$.

a) Si determini il campo di spezzamento K di f su $\mathbb{Z}_3$.

b) Si stabilisca se in K esiste un elemento il cui quadrato é $[2]_3$.

c) Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani e si consideri il suo ideale $I = (3)$. Si stabilisca se $\mathbb{Z}[i]/I$ é un campo e se é isomorfo a K.

Informatico-Computazionale A.A. 2005–06

Prova scritta di Algebra II (M. Manaresi) – 18.7.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi eccetto il punto 2e).

Esercizio 1. Sia $\mathbb{Z}_4 \times \mathbb{Z}_6$ il gruppo prodotto diretto dei gruppi additivi $\mathbb{Z}_4$ e $\mathbb{Z}_6$ delle classi di resto modulo 4 e 6 rispettivamente.

a) Elencare gli omomorfismi di gruppi da $\mathbb{Z}_9$ a $\mathbb{Z}_4 \times \mathbb{Z}_6$.
b) Esiste un omomorfismo di gruppi f_1 da $\mathbb{Z}_9$ a $\mathbb{Z}_4 \times \mathbb{Z}_6$ tale che $Im(f_1)$ abbia 8 elementi?
c) Esiste un omomorfismo di gruppi f_2 da $\mathbb{Z}_9$ a $\mathbb{Z}_4 \times \mathbb{Z}_6$ tale che $Ker(f_2)$ sia il sottogruppo $< [3]_9 >$ di $\mathbb{Z}_9$?

Esercizio 2. Sia $\mathbb{Q}[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Q}$ dei numeri razionali, siano $f = x^4 + x^3 - 5x^2 - 4x + 4$ e $g = x^4 - 9x^2 + 20$ due suoi elementi, sia $I = (f, g)$ e sia $A := \mathbb{Q}[x]/I$ l'anello quoziente di $\mathbb{Q}[x]$ rispetto all'ideale I.

a) Stabilire se il laterale $I + x^5 + x + 2$ contiene un polinomio lineare.
b) Stabilire se i laterali $I + x$ e $I + g$ sono elementi invertibili dell'anello quoziente A, e, in caso affermativo, determinare i loro inversi.
c) Stabilire se nell'anello quoziente A esistono elementi il cui quadrato é zero.
d) Determinare il campo di spezzamento K di f su $\mathbb{Q}$ e stabilire se su K anche g si spezza in fattori lineari.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{R}$ i campi dei razionali e dei reali rispettivamente, siano u_1, u_2 le radici nel campo complesso del polinomio $f = x^2 + \sqrt{2}x - 1 \in \mathbb{R}[x]$.

a) Determinare i polinomi minimi di u_1, u_2 su $\mathbb{Q}$.

b) Stabilire se $u_2 \in \mathbb{Q}(u_1)$.

c) Mostrare che $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(u_2)$ e calcolare $[\mathbb{Q}(u_2) : \mathbb{Q}(\sqrt{2})]$.

d) Stabilire se esisrte qualche relazione di inclusione tra i campi $\mathbb{Q}(u_1)$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani, sia $I = (2 + i)$ un suo ideale; sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$, sia $f = x^2 + x + 1$ un suo elemento e sia $K = \mathbb{Z}_5[x]/(f)$ l'anello quoziente.

a) Provare che gli anelli $\mathbb{Z}[i]/I$ e K sono campi e calcolarne la caratteristica.
b) Stabilire se i campi $\mathbb{Z}[i]/I$ e K sono isomorfi.
c) Stabilire se nell'anello K risulta $([x]_{(f)})^{25} = [x]_{(f)}$.

Informatico-Computazionale A.A. 2005–06

Prova scritta di Algebra II (M. Manaresi) – 13.9.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $G = \mathbb{Z}_3 \times \mathbb{Z}_4$ il gruppo prodotto diretto dei gruppi additivi $\mathbb{Z}_3$ e $\mathbb{Z}_4$ delle classi di resto modulo 3 e 4 rispettivamente.

a) Stabilire quanti sono gli omomorfismi di gruppi dal gruppo G al gruppo S_4 delle permutazioni su quattro lettere. [Suggerimento: ricordare che il gruppo G é ciclico.]
b) Esiste un omomorfismo di gruppi iniettivo f_1 da G a S_4?
c) Esiste un omomorfismo di gruppi f_2 da G a S_4 tale che $Ker(f_2)$ sia il sottogruppo $< ([0]_3, [1]_4) >$ di G?

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti nell'anello $\mathbb{Z}$ dei numeri interi, siano $A := \mathbb{Z}[x]/(x^2)$ e $B := \mathbb{Z}[x]/(x^2, 14)$ gli anelli quoziente di $\mathbb{Z}[x]$ rispetto agli ideali (x^2) e $(x^2, 14)$ rispettivamente; sia $C := \mathbb{Z}_{14}[x]/(x^2)$ l'anello quoziente di $\mathbb{Z}_{14}[x]$ rispetto all'ideale (x^2).

a) Stabilire se gli anelli A, B e C sono finiti o infiniti.
b) Determinare i divisori di zero dell'anello A.
c) Stabilire se il polinomio $x^4 + 7x^2 + 6x - 9 \in [x^5 + 2x^3 - 8x + 5]_{(x^2,14)}$.
d) Stabilire se l'anello B é un quoziente dell'anello A e se gli anelli quoziente $B = \mathbb{Z}[x]/(x^2, 14)$ e $C := \mathbb{Z}_{14}[x]/(x^2)$ sono isomorfi.

Esercizio 3. Sia $\mathbb{Q}$ il campo dei razionali, sia $L := \mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{3})$.

a) Provare che $[L : Q]$ é divisibile per 3 e per 4.

b) Provare che $[L : Q] \leq 12$ e dedurre da a) che $[L : Q] = 12$.

d) Sia K il campo di spezzamento del polinomio $(x^4 - 2)(x^3 - 3)$. Stabilire se $K = L$ o se fra i due campi esiste qualche relazione di inclusione.

Esercizio 4.

a) Stabilire se il campo $\mathbb{Z}_2[x]/(x^3 + x + 1)$ ha un sottocampo isomorfo a $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

b) Individuare un sottocampo del campo $\mathbb{Z}_2[x]/(x^4 + x^2 + 1)$ isomorfo al campo $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

a) Stabilire se il campo $\mathbb{Z}_2[x]/(x^4 + x^2 + 1)$ ha un sottoanello isomorfo all'anello $\mathbb{Z}[i]/(1 + 7i, 3 + 3i)$ (dove $\mathbb{Z}[i]$ é l'anello degli interi gaussiani).

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Esercitazione scritta di Algebra II (M. Manaresi) – 15.12.06

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi con esclusione del punto **2d**.

Esercizio 1. Sia $G = S_5 \times \mathbb{Z}_4$ il gruppo prodotto diretto dei gruppi S_5 e $\mathbb{Z}_4$.

a) Stabilire se gli elementi $((135), [2]_4), ((234), [1]_4) \in G$ sono coniugati in G.
b) Scrivere due sottogruppi propri H e L di G tali che H sia normale in G, mentre L non sia normale in G.
c) Stabilire se esistono due diversi omomorfismi iniettivi da $\mathbb{Z}_6$ a $G = S_5 \times \mathbb{Z}_4$. Nel caso esistano, per ognuno calcolare l'immagine.

Esercizio 2. Sia $\mathbb{Z}_7[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_7$, siano $f = x^5 + [4]_7x^3 + x^2 + [3]_7 + [3]_7$ e $g = x^4 + [2]_7x^2 + [4]_7$ due suoi elementi, siano $I = (f)$, $J = (f, g)$ e siano $A := \mathbb{Z}_7[x]/I$, $B := \mathbb{Z}_7[x]/J$ gli anelli quoziente dell'anello $\mathbb{Z}_7[x]$, rispetto agli ideali I e J rispettivamente.

a) Stabilire se gli anelli A e B sono domini d'integritá.
b) Stabilire se nell'anello $\mathbb{Z}_7[x]$ esistono due polinomi $r(x)$ e $s(x)$ tali che valga la relazione $r(x)f(x) + s(x)g(x) = x + 2$.
c) Stabilire se l'applicazione $\sigma : A := \mathbb{Z}_7[x]/I \to B := \mathbb{Z}_7[x]/J$, data da $\sigma([h]_I) = [h]_J$, é ben definita e se é un omomorfismo di anelli. In caso affermativo stabilire se $[x + 1]_I \in Ker\,\sigma$ e se $[x + 1]_J \in Im\,\sigma$.
d) Determinare il campo si spezzamento K del polinomio g su $\mathbb{Z}_7[x]$ e stabilire se il polinomio f si spezza in fattori lineari su K.

Esercizio 3. Sia $u \in \mathbb{C}$ una delle radici complesse del polinomio $f = x^3 + 3x + 2 \in \mathbb{Q}[x]$.

a) Provare che $\mathbb{Q}(u) = \mathbb{Q}(u^2)$.
b) Scrivere gli elementi u^3 e $\dfrac{1}{u+1}$ di $\mathbb{Q}(u)$ nella forma au^2+bu+c con $a, b, c \in \mathbb{Q}$.
c) Sia g un polinomio di grado 4 irriducibile su $\mathbb{Q}$. E' vero che g é anche irriducibile su $\mathbb{Q}(u)$?

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss e per ogni $t \in \mathbb{N}$ sia $w_t \in \mathbb{Z}[i]$ l'elemento definito da $w_t = t + 6 + (3t - 2)i$.

a) Verificare che $w_t \in (3 - i)$ per ogni $t \in \mathbb{N}$.
b) Trovare un generatore dell'ideale $I = (w_1) + (w_3)$ e stabilire se l'ideale é primo.
c) Stabilire se esiste un omomorfismo suriettivo dall'anello quoziente $A = \mathbb{Z}[i]/I$ nel campo $K = \mathbb{Z}[i]/(2 + i)$.

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Prova scritta di Algebra II (M. Manaresi) – 9.1.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia S_4 il gruppo delle permutazioni su 4 lettere e sia H il suo sottogruppo definito da $H := \{\alpha \in S_4 \ / \ \alpha(\{1,2\}) = \{1,2\}\}$.

a) Stabilire se H é un sottogruppo normale di S_4 e, qualora non lo sia, scrivere un sottogruppo coniugato $C_\beta(H)$ di H (con $\beta \in S_4$) tale che $C_\beta(H) \neq H$.
b) Stabilire (motivando la risposta) se esistono omomorfismi di gruppi iniettivi $\mathbb{Z}_m \to S_4$ per $m = 2, 3, 4, 6, 8, 10, 12$.

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi e siano $I_1 = (x^2+2)$, $I_2 = (x^2+3x+2)$, $I_3 = (x^2, 2)$, $I_4 = (x+2)$ e $I_5 = (x, 2)$ cinque suoi ideali.

a) Stabilire se esistono relazioni di inclusione fra gli ideali I_1, I_2, I_3, I_4, I_5, quali di questi ideali sono primi e quali sono massimali.
b) Stabilire se l'ideale I_3 é principale.
c) Determinare gli ideali somma $I_1 + I_k$ per $k = 3, 4, 5$.
d) Sia $A := \mathbb{Z}[x]/I_1$ l'anello quoziente dell'anello $\mathbb{Z}[x]$ rispetto all'ideale I_1 e sia $\pi : \mathbb{Z}[x] \to A := \mathbb{Z}[x]/I_1$ la proiezione sul quoziente. Stabilire se $\pi(I_3)$, $\pi(I_4)$, $\pi(I_5)$ sono ideali distinti dell'anello A o se alcuni di essi coincidono.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei numeri razionali e dei numeri complessi rispettivamente, $u = \sqrt{2}/(1+i)$ e $\sigma_u : \mathbb{Q}[x] \to \mathbb{C}$ il relativo morfismo sostituzione.
a) Stabilire se u appartiene a $\mathbb{Q}(\sqrt{2})$.
b) Stabilire se $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(u)$.
c) Stabilire se $Im\ \sigma_u = \{q_1 + q_2 u \ / \ q_1, q_2 \in \mathbb{Q}\}$.
d) Stabilire se esistono $a, b \in \mathbb{Q}$ per i quali il polinimio $ax^2 + b$ appartiene a $ker\ \sigma_u$.
e) Stabilire se il campo di spezzamento K del polinomio minimo p_u di u su $\mathbb{Q}$ coincide con il campo $\mathbb{Q}(\sqrt{2}, i)$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani e sia $v = 41 + 23i \in \mathbb{Z}[i]$.

a) Decomporre v in irriducibili di $\mathbb{Z}[i]$.
b) Determinare un elemento $w \in \mathbb{Z}[i]$ tale che l'ideale $I = (v, w) \subset \mathbb{Z}[i]$ sia massimale ed esista un omomorfismo di campi $\mathbb{Z}_5 \to \mathbb{Z}[i]/I$.
c) Determinare due ideali I_1 e I_2 di $\mathbb{Z}[i]$ tali che $I_1 \subset (v) \subset I_2$ (inclusioni strette).

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Prova scritta di Algebra II (M. Manaresi) – 7.2.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia S_4 il gruppo delle permutazioni su 4 lettere e S_5 il gruppo delle permutazioni su 5 lettere. Siano $\alpha = (12)(34)$, $\beta = (13)(24)$ e siano H e K i sottogruppi di S_4 e S_5 rispettivamente generati da $\{\alpha, \beta\}$.

a) Stabilire se H é un sottogruppo normale di S_4.
b) Stabilire se K é un sottogruppo normale di S_5.
c) Stabilire se i cicli (1345) e (1352) stanno nello stesso laterale di K in S_5.
d) Sia $f : S_4 \to S_5$ l'omomorfismo di gruppi che associa ad ogni permutazione $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{pmatrix} \in S_4$ la permutazione $f(\alpha) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) & 5 \end{pmatrix} \in S_5$. Sia $L =< (12), (3,4,5) > \subset S_5$. Si determini il sottogruppo $f^{-1}(L) \subset S_4$.

Esercizio 2. Siano $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ gli anelli dei polinomi a coefficienti interi e a coefficienti razionali rispettivamente, siano $f(x) = x^2 + ax + 1$ con $a \in \mathbb{Z}$, $g(x) = x + 2$ due polinomi di $\mathbb{Z}[x]$ e si considerino gli ideali somma $I = (f) + (g) \subset \mathbb{Z}[x]$, $J = (f) + (g) \subset \mathbb{Q}[x]$.

a) Stabilire se esiste un $a \in \mathbb{Z}$ tale che l'anello quoziente $\mathbb{Q}[x]/J$ sia un campo.
b) Stabilire se esiste un $a \in \mathbb{Z}$ tale che l'anello quoziente $\mathbb{Z}[x]/I$ non sia l'anello nullo e abbia dei divisori di zero non nulli.
c) Sia $a = 1$ e sia $\psi : \mathbb{Z}[x] \to \mathbb{Z}_3$ l'omomorfismo di anelli definito da $\psi(f(x)) = [f(-2)]_3$ per ogni $f(x) \in \mathbb{Z}[x]$. Si determinino il nucleo e l'immagine di ψ.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei numeri razionali e dei numeri complessi rispettivamente, sia $f = x^6 - 3x^3 + 2 \in \mathbb{Q}[x]$.

a) Determinare il campo di spezzamento K del polinomio f su $\mathbb{Q}$ e calcolare il grado dell'estensione $[K : \mathbb{Q}]$.
b) Sia $u \in \mathbb{C}$ una radice complessa di f tale che $u^3 \neq 1$. Si stabilisca se nel campo $\mathbb{Q}(u)$ vale la relazione $u^7 = 4u$ e si scriva l'inverso dell'elemento $u^2 + u + 1$.

Esercizio 4. Siano $f_1 = x^2 + x + 1, f_2 = x^3 + x + 1$ polinomi di $\mathbb{Z}_2[x]$ e sia $f = f_1 f_2$. Siano K_1 il campo di spezzamento di f_1 su $\mathbb{Z}_2$, K_2 il campo di spezzamento di f_2 su $\mathbb{Z}_2$, K il campo di spezzamento di f su $\mathbb{Z}_2$.

a) Stabilire se il polinomio f_2 ammette una radice in K_1.
b) Determinare il grado dell'estensione $\mathbb{Z}_2 \subset K$.
c) Determinare la caratteristica dell'anello $K_1 \times K_2$ e stabilire se si puó definire un omomorfismo di anelli iniettivo da $K_1 \times K_2$ a K.
d) Determinare un elemento v dell'"anello degli interi di gaussiani $\mathbb{Z}[i]$ tale che $\mathbb{Z}[i]/(v)$ sia un campo e si possa definire un omomorfismo di anelli $\mathbb{Z}[i]/(v) \to K_1$.

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Prova scritta di Algebra II (M. Manaresi) – 6.6.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\mathbb{Z}_{15}^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{15}$ delle classi di resto modulo 15 e sia $\mathbb{Z}_m$ il gruppo additivo delle classi di resto modulo m.

a) Stabilire per quali valori di m esiste un omomorfismo di gruppi diverso dall'omomorfismo banale da $\mathbb{Z}_m$ a $\mathbb{Z}_{15}^*$.
b) Stabilire per quali valori di m esistono omomorfismi di gruppi iniettivi da $\mathbb{Z}_m$ a $\mathbb{Z}_{15}^*$.
c) Stabilire per quali valori di m esistono omomorfismi di gruppi suriettivi da $\mathbb{Z}_m$ a $\mathbb{Z}_{15}^*$.

Esercizio 2. Siano $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ gli anelli dei polinomi a coefficienti interi e a coefficienti razionali rispettivamente, siano $f(x) = x^3 - 2x - 1$ $g_a(x) = x + a$, con $a \in \mathbb{Z}$, due polinomi di $\mathbb{Z}[x]$ e si considerino gli ideali somma $I_a = (f) + (g_a) \subset \mathbb{Z}[x]$, $J_a = (f) + (g_a) \subset \mathbb{Q}[x]$.

a) Stabilire se esiste un $a \in \mathbb{Z}$ tale che l'ideale $I_a \subset \mathbb{Z}[x]$ sia principale.
b) Stabilire se esiste un $a \in \mathbb{Z}$ tale che l'anello quoziente $\mathbb{Z}[x]/I_a$ sia un campo.
c) Determinare tutti gli $a \in \mathbb{Z}$ tali che l'anello quoziente $\mathbb{Q}[x]/J_a$ è un campo.
d) Sia $a = 2$ e sia $\psi : \mathbb{Z}[x] \to \mathbb{Z}_3$ l'omomorfismo di anelli definito da $\psi(f(x)) = [f(-2)]_3$ per ogni $f(x) \in \mathbb{Z}[x]$. Si stabilisca se l'omomorfismo ψ è suriettivo e se ne calcoli il nucleo.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{-3})$ rispettivamente il campo dei numeri razionali e la sua estensione con l'aggiunta di $\sqrt{-3}$: Sia $u = \epsilon \sqrt[3]{5}$, ove $\epsilon \neq 1$ è una radice terza primitiva complessa di 1 (cioè $\epsilon^3 = 1$).

a) Si calcoli il polinomio minimo p_ϵ di ϵ su $\mathbb{Q}$.
b) Si provi che u è algebrico su $\mathbb{Q}$ e si calcoli il polinomio minimo p_u di u su $\mathbb{Q}$.
c) Si determini il campo si spezzamento del polinomio p_u su $\mathbb{Q}$. [Suggerimento: utilizzando il punto a) si provi che $\epsilon \notin \mathbb{Q}(u)$.]
d) Si consideri ora $p_u \in \mathbb{Q}(\sqrt{-3})[x]$. Si provi che p_u è irriducibile su $\mathbb{Q}(\sqrt{-3})$ e si stabilisca se il campo di spezzamento di p_u su $\mathbb{Q}(\sqrt{-3})$ coincide con il campo si spezzamento di p_u su $\mathbb{Q}$.

Esercizio 4. Nell'anello degli interi di Gauss $Z[i]$ siano $u = 2i + 6$ e $v = 9i - 3$.

a) Si determini un generatore dell'ideale $I = (u) + (v)$, si stabilisca se tale ideale é massimale e si calcoli la caratteristica dell'anello quoziente $\mathbb{Z}[i]/I$.
b) Si stabilisca se esistono primi p per i quali l'anello quoziente $\mathbb{Z}[i]/I$ contiene un sottocampo isomorfo a $\mathbb{Z}_p$.
c) Si stabilisca se esistono primi p per i quali é possibile definire un omomorfismo di anelli suriettivo da $\mathbb{Z}[i]/I$ al campo $\mathbb{Z}_p$.

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Prova scritta di Algebra II (M. Manaresi) – 10.7.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\mathbb{Z}_8$ il gruppo additivo delle classi di resto modulo 8 e sia $(\mathbb{Z}_{14} \times \mathbb{Z})^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{14} \times \mathbb{Z}$ prodotto diretto dell'anello $\mathbb{Z}_{14}$ delle classi di resto modulo 14 e dell'anello $\mathbb{Z}$ degli interi .

a) Stabilire quanti sono gli omomorfismi di gruppi da $\mathbb{Z}_8$ a $(\mathbb{Z}_{14} \times \mathbb{Z})^*$.
b) Stabilire se esistono omomorfismi di gruppi suriettivi da da $\mathbb{Z}_8$ a $(\mathbb{Z}_{14} \times \mathbb{Z})^*$.
c) Stabilire se esistono omomorfismi di gruppi $f : \mathbb{Z}_8 \to (\mathbb{Z}_{14} \times \mathbb{Z})^*$ tali che $Ker f =< [4]_8 >$.
d) E' vero che se $f : \mathbb{Z}_8 \to (\mathbb{Z}_{14} \times \mathbb{Z})^*$ é un omomorfismo di gruppi tale che $([-1]_{14}, 1) \in \Im f$ allora $Ker f =< [2]_8 >$?

Esercizio 2. Sia $\mathbb{Z}_7[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_7$ delle classi di resto modulo 7 , sia $I := (x^3 + 5x + 1)$, sia $A := \mathbb{Z}_7[x]/I$ l'anello quoziente e sia $\pi : \mathbb{Z}_7[x] \to A$ la proiezione canonica sul quoziente.

a) Stabilire quanti sono gli elementi dell'anello A e se in tale anello ci sono divisori dello zero non nulli.
b) Elencare gli ideali massimali M dell'anello A e per ognuno determinare la caratteristica e il numero degli elementi dell'anello quoziente A/M .
c) Determinare un ideale proprio J di $\mathbb{Z}_7[x]$ tale che $\pi(J)$ sia un ideale proprio di A .
d) Si considerino gli ideali $J_1 = (x+2)$ e $J_2 = (x^2+6x+8)$ di $\mathbb{Z}_7[x]$ e si stabilisca se $\pi(J_1) = \pi(J_2)$.

Esercizio 3. Siano u , v due numeri complessi che doddisfano le condizioni $u^2 - 6u = -1, v^2 - v = u$,.

a) Si provi che v é algebrico e si determini il suo polinomio minimo p_v su $\mathbb{Q}$.
b) Si provi che $\mathbb{Q}(u)$ è contenuto propriamente in $\mathbb{Q}(v)$?
c) E' vero che $v - 1$ é radice di p_v ?

Esercizio 4. Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ siano $u = 15 - 5i$, $v = 1 + 17i$ e sia $A := \mathbb{Z}[i]/(u, v)$. Sia K un campo.

a) Esiste un sottoanello di K isomorfo ad A ?
b) Esiste un campo K per il quale é possibile definire un omomorfismo di anelli $\sigma : A \to K$?
c) Esiste un campo K per il quale é possibile definire un omomorfismo di anelli $\psi : K \to A$?

Università di Bologna C.d.L. in Matematica A.A. 2006–07

Prova scritta di Algebra II (M. Manaresi) – 12.9.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1. Sia $\mathbb{Z}_8$ il gruppo additivo delle classi di resto modulo 8 e sia $(\mathbb{Z}_{14} \times \mathbb{Z})^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{14} \times \mathbb{Z}$ prodotto diretto dell'anello $\mathbb{Z}_{14}$ delle classi di resto modulo 14 e dell'anello $\mathbb{Z}$ degli interi .

a) Stabilire quanti sono gli omomorfismi di gruppi da $\mathbb{Z}_8$ a $(\mathbb{Z}_{14} \times \mathbb{Z})^*$.
b) Stabilire se esistono omomorfismi di gruppi suriettivi da da $\mathbb{Z}_8$ a $(\mathbb{Z}_{14} \times \mathbb{Z})^*$.
c) Stabilire se esistono omomorfismi di gruppi $f : \mathbb{Z}_8 \to (\mathbb{Z}_{14} \times \mathbb{Z})^*$ tali che $Ker f = < [4]_8 >$.
d) E' vero che se $f : \mathbb{Z}_8 \to (\mathbb{Z}_{14} \times \mathbb{Z})^*$ é un omomorfismo di gruppi tale che $([-1]_{14}, 1) \in \Im f$ allora $Ker f = < [2]_8 >$?

Esercizio 2. Sia $\mathbb{Z}_7[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_7$ delle classi di resto modulo 7, sia $I := (x^3 + 5x + 1)$, sia $A := \mathbb{Z}_7[x]/I$ l'anello quoziente e sia $\pi : \mathbb{Z}_7[x] \to A$ la proiezione canonica sul quoziente.

a) Stabilire quanti sono gli elementi dell'anello A e se in tale anello ci sono divisori dello zero non nulli.
b) Elencare gli ideali massimali M dell'anello A e per ognuno determinare la caratteristica e il numero degli elementi dell'anello quoziente A/M.
c) Determinare un ideale proprio J di $\mathbb{Z}_7[x]$ tale che $\pi(J)$ sia un ideale proprio di A.
d) Si considerino gli ideali $J_1 = (x+2)$ e $J_2 = (x^2+6x+8)$ di $\mathbb{Z}_7[x]$ e si stabilisca se $\pi(J_1) = \pi(J_2)$.

Esercizio 3. Siano u, v due numeri complessi che doddisfano le condizioni $u^2 - 6u = -1, v^2 - v = u$,.
a) Si provi che v é algebrico e si determini il suo polinomio minimo p_v su $\mathbb{Q}$.
b) Si provi che $\mathbb{Q}(u)$ è contenuto propriamente in $\mathbb{Q}(v)$?
c) E' vero che $v - 1$ é radice di p_v ?

Esercizio 4. Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ siano $u = 15 - 5i$, $v = 1 + 17i$ e sia $A := \mathbb{Z}[i]/(u, v)$. Sia K un campo.

a) Esiste un sottoanello di K isomorfo ad A?
b) Esiste un campo K per il quale é possibile definire un omomorfismo di anelli $\sigma : A \to K$?
c) Esiste un campo K per il quale é possibile definire un omomorfismo di anelli $\psi : K \to A$?

Università di Bologna **C.d.L. in Matematica A.A. 2006–07**

Prova scritta di Algebra II (M. Manaresi) – 13.12.07

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere il primo esercizio e i punti a), b), c) del secondo esercizio.

Esercizio 1. Sia S_5 il gruppo delle permutazioni su 5 lettere, siano $H := \{\alpha \in S_5 \,|\, \alpha(\{1,2,3\}) = \{1,2,3\}\}$, $K := \{\alpha \in S_5 | \alpha(\{1,2\}) = \{1,2\},\ \alpha(3) = 3\}$.

a) Si scrivano gli elementi di H e di K e se ne calcolino i periodi.
b) Si stabilisca se H é un sottogruppo normale di S_5 e se K é un sottogruppo normale di H.
c) Si stabilisca se H e K sono gruppi ciclici o se sono isomorfi a gruppi prodotto $\mathbb{Z}_m \times \mathbb{Z}_n$ per opportuni m, n (eventualmente uguali).
d) Si stabilisca per quali interi positivi m esiste un omomorfismo di gruppi non banale $\mathbb{Z}_m \to K$.

Esercizio 2. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$ delle classi di resto modulo 5, sia $I := (x^3 + 3x^2 + 2x + 1)$, sia $A := \mathbb{Z}_5[x]/I$ l'anello quoziente e sia $\pi : \mathbb{Z}_5[x] \to A$ la proiezione canonica sul quoziente.

a) Si stabilisca se l'anello quoziente é un dominio d'integritá e calcolarne la caratteristica.
b) Si stabilisca se nell'anello A l'elemento $[x-1]_I$ é invertibile e, in caso positivo, calcolarne l'inverso.
c) Si stabilisca se nell'anello A l'ideale $\pi((x^4 - 1))$ é proprio.
d) Elencare tutti i campi K per i quali é definito un omomorfismo suriettivo $A \to K$ e stabilire se tali campi sono tutti tra loro isomorfi.
e) Sia K un campo di cui al punto e) e sia L un campo che contenga K come sottocampo e sia un K-spazio vettoriale di dimensione finita. Il campo L é necessariamente finito?
f) Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss, siano $u = 15 - 5i$, $v = (2a+1) + (2-a)i$, con $a \in \mathbb{Z}$, due suoi elementi. E' possibile determinare $a \in \mathbb{Z}$ in modo che l'anello $B := \mathbb{Z}[i]/(u, v)$ sia un campo ed esista un omomorfismo di anelli $\mathbb{Z}_5 \to B$?

Esercizio 3. Siano $f_1 = x^5 - 2x^3 + x^2 - 2$, $f_2 = x^4 - x^3 - 2x^2 - 3x - 1$, $f_3 = x^4 - 4x^2 + 2$.

a) Determinare la decomposizione di f_1, f_2, f_3 in irriducibili di $\mathbb{Q}[x]$.
b) Determinare i campi di spezzamento L_1, L_2, L_3 di f_1, f_2, f_3 (rispettivamente) su $\mathbb{Q}$ e stabilire se essi sono isomorfi come $\mathbb{Q}$-spazi vettoriali.
c) Si stabilisca se tra i campi L_1, L_2, L_3 esistono relazioni di inclusione.
d) Si stabilisca se esiste un campo K contenuto in $L_1 \cap L_2 \cap L_3$ che é estensione propria di $\mathbb{Q}$.

Università di Bologna **C.d.L. in Matematica A.A. 2006–07**

Prova scritta di Algebra II (M. Manaresi) – 8.1.08

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi, con l'esclusione di 2.f).

Esercizio 1. Sia $\mathbb{Z} \times \mathbb{Z}$ il gruppo prodotto diretto del gruppo degli interi per se stesso e siano H e K i seguenti sottogruppi di $\mathbb{Z} \times \mathbb{Z}$:

$$H = < (4,10) >, \quad K = < 4 > \times < 10 > .$$

a) Stabilire se i laterali $H + (9,9)$ e $H + (29,29)$ di H sono uguali.
b) Stabilire se i laterali $K + (9,9)$ e $K + (29,29)$ di K sono uguali.
c) Stabilire se i gruppi quoziente $\mathbb{Z} \times \mathbb{Z}/H$ e $\mathbb{Z} \times \mathbb{Z}/K$ sono finiti o infiniti.
d) Stabilire se esiste un omomorfismo di gruppi suriettivo da $\mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}/K$.

Esercizio 2. Sia $\mathbb{Q}[x]$ l'anello dei polinomi a coefficienti nel campo dei numeri razionali, sia $I := (x^4 - 2x^3 - x + 2)$, sia $A := \mathbb{Q}[x]/I$ l'anello quoziente e sia $\pi : \mathbb{Q}[x] \to A$ la proiezione canonica sul quoziente.

a) Stabilire per quali valori di $a \in \mathbb{Z}$ l'ideale somma $(x^2 + ax + 2) + I \subset \mathbb{Q}[x]$ contiene polinomi di grado 1.
b) Stabilire se nell'anello A l'elemento $[x + 2]_I$ é invertibile e, in caso positivo, calcolarne l'inverso.
c) Stabilire se nell'anello A l'ideale $\pi((x^4 - 1))$ é proprio.
d) Provare che S é un ideale primo dell'anello quoziente A se e solo se l'ideale $\pi^{-1}(S)$ é primo in A.
e) Elencare gli ideali dell'anello A stabilendo quali sono ideali primi e quali sono massimali.
f) Si determini il campo di spezzamento K del polinomio $x^4 - 2x^3 - x + 2$ su $\mathbb{Q}$ e si stabilisca se é possibile definire un omomorfismo di anelli suriettivo $A \to K$.

Esercizio 3. Sia $u = \sqrt{3 - \sqrt{5}} \in \mathbb{R}$.

a) Stabilire se u é un elemento di $\mathbb{Z}[\sqrt{5}]$.
b) Provare che u é algebrico su $\mathbb{Q}$ e determinare il polinomio minimo p_u di u su $\mathbb{Q}$.
c) Mostrare che $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(u)$ e determinare la fattorizzazione di p_u in irriducibili di $\mathbb{Q}(\sqrt{5})[x]$.
d) Calcolare il polinomio minimo q_u di u su $\mathbb{Q}(\sqrt{5})$.
e) Stabilire se il campo di spezzamento di p_u su $\mathbb{Q}$ é un'estensione semplice di $\mathbb{Q}$.

Esercizio 4. Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ siano $u = 7 + 6i$, $v = 8 - i$.

a) Stabilire se esiste un omomorfismo di anelli iniettivo dal campo $\mathbb{Z}_3$ nell'anello quoziente $A := \mathbb{Z}[i]/(u, v)$.
b) Stabilire se esiste un omomorfismo di anelli suriettivo dal campo di Galois di ordine 25 all'anello quoziente $A := \mathbb{Z}[i]/(u, v)$.

Università di Bologna **C.d.L. in Matematica A.A. 2006–07**

Prova scritta di Algebra II (M. Manaresi) – 7.2.08

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere i primi due esercizi.

Esercizio 1.

a) Stabilire quanti sono gli omomorfismi di gruppi da $\mathbb{Z}_{10}$ a $\mathbb{Z}_{40}$ e da $\mathbb{Z}_{40}$ a $\mathbb{Z}_{10}$ e quali di essi sono anche omomorfismi di anelli.

b) Stabilire se esistono omomorfismi di gruppi $\phi : \mathbb{Z}_{40} \to \mathbb{Z}_{10}$ per i quali risulta $\ker \phi = < [5]_{40} >$.

c) Esiste un gruppo quoziente del gruppo prodotto diretto $\mathbb{Z}_{10} \times \mathbb{Z}_{40}$ con 16 elementi? Se sí, come si puó ottenere?

d) Stabilire per quali n esistono omomorfismi di gruppi da $\mathbb{Z}_{10}$ al gruppo delle permutazioni S_n, con $n \geq 1$, e se fra essi vi sono degli omomorfismi suriettivi.

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, siano $I_1 := (x^2, x + 6, 3)$, $I_2 := (2x^2, 3), I_3 := (x^4 - 2x^3 - x + 2, x^2, 3)$ tre suoi ideali.

a) Stabilire se gli ideali I_1, I_2, I_3 sono principali e se fra essi sussistono relazioni di inclusione.

b) Stabilire se tra gli ideali I_1, I_2, I_3 ve ne sono di primi e di massimali.

c) Stabilire se l'anello quoziente $\mathbb{Z}[x]/I_2$ contiene un elemento invertibile.

d) Stabilire se l'immagine dell'ideale I_3 attraverso la proiezione canonica $\pi : \mathbb{Z}[x] \to \mathbb{Z}[x]/I_2$ é un ideale proprio dell'anello quoziente $\mathbb{Z}[x]/I_2$ diverso dall'ideale nullo.

Esercizio 3. Sia $\xi = e^{2\pi i/6} \in \mathbb{C}$ una radice n-esima primitiva dell'unitá; siano $f_1 = x^6 - 2$ e $f_2 = (x^2 - 2)(x^3 - 3)$ due polinomi di $\mathbb{Q}[x]$, K_1 e K_2 i loro campi di spezzamento su $\mathbb{Q}$.

a) Provare che ξ é algebrico su $\mathbb{Q}$ e determinarne il suo polinomio minimo p_ξ su $\mathbb{Q}$.

b) Determinare il campo di spezzamento L di p_ξ su $\mathbb{Q}$, calcolare $[L : \mathbb{Q}]$ e stabilire se $L = \mathbb{Q}(\xi)$.

c) Scrivere una base di K_1 e una base di K_2 come $\mathbb{Q}$-spazi vettoriali e stabilire se i due campi sono $\mathbb{Q}$-spazi vettoriali isomorfi.

d) Stabilire se $\xi \in K_1 \cap K_2$.

Esercizio 4. Sia $\mathbb{Z}_2[x]$ l'anello dei polinomi a coefficienti nell'anello $\mathbb{Z}_2$ delle classi di resto modulo 2 e sia $f = x^3 + x + 1$ un suo elemento.

Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss e siano $u = 9 + 3i$ $v = -8 + 22i$ due suoi elementi.

a) Si provi che $K = \mathbb{Z}_2[x]/(f)$ é un campo, si scrivano esplicitamente i suoi elementi e si stabilisca se su K il polinomio f si spezza in fattori lineari.

b) Si stabilisca se in K vi sono elementi che non sono quadrati e se esiste un omomorfismo di anelli iniettivo dal campo di Galois di ordine 4 a K.

c) Si stabilisca se esiste un omomorfismo di anelli iniettivo dall'anello quoziente $A := \mathbb{Z}[i]/(u, v)$ al campo K.

Università di Bologna **C.d.L. in Matematica A.A. 2007–08**

Prova scritta di Algebra II (M. Manaresi) – 28.05.08

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere il primo esercizio e i punti a), b), c) del secondo esercizio.

Esercizio 1. Sia S_6 il gruppo delle permutazioni su 6 lettere, siano $\alpha = (1324)$, $\beta = (12)(3456)$ due elementi di S_6 e siano $H =< \alpha >$ e $K =< \beta >$ i sottogruppi di S_6 generati dai due elementi.

a) Stabilire se H e K sono sottogruppi normali di S_6.
b) Stabilire se esiste un elemento $\gamma \in S_6$ tale che $C_\gamma(H) = K$, dove C_γ denota il coniugio rispetto a γ.
c) Stabilire se esiste un omomorfismo di gruppi $f : S_6 \to S_6$ tale che $\ker f = H$.
d) Stabilire per quali $m \in \mathbb{Z}, m > 1$, esiste un omomorfismo di gruppi $h : \mathbb{Z}_m \to S_6$ tale che $Im\, h = K$.

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, siano $I := (x^3 - 2x + 5, x^2 - 2x + 1)$ e $J := (x + 1, 2)$ due suoi ideali, sia $A := \mathbb{Z}[x]/I$ l'anello quoziente.

a) Stabilire se l'ideale J é un ideale massimale di $\mathbb{Z}[x]$ e se contiene l'ideale I.
b) Stabilire se l'anello A é un dominio d'integritá e calcolarne la caratteristica.
c) Determinare la cardinalitá dell'anello A e la cardinalitá dell'insieme dei suoi elementi invertibili.

Esercizio 3. Sia $\mathbb{Q}$ il campo dei numeri razionali, sia $u = 1 + \sqrt[3]{5}\, e^{2\pi i/3}$ e sia $\sigma_u : \mathbb{Q}[x] \to \mathbb{C}$ l'omomorfismo sostituzione.

a) Provare che u é algebrico su $\mathbb{Q}$, determinandone il polinomio minimo p_u e calcolando $[\mathbb{Q}(u) : \mathbb{Q}]$.
b) Stabilire se $u \in \mathbb{Q}(\sqrt[3]{5})$ e se $u \in \mathbb{Q}(e^{2\pi i/3})$.
c) Stabilire se esistono $a, b \in \mathbb{Q}$ per i quali il polinomio $ax + b \in \ker \sigma_u$.
d) Determinare il campo di spezzamento K di p_u su $\mathbb{Q}$ e stabilire se $K = \mathbb{Q}(u)$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss e siano $u = 12+5i$, $v = 7+4i$, $w = 3 - 5i$ tre suoi elementi.

a) Stabilire se esiste una relazione di inclusione fra gli ideali $I = (u) \cap (v)$, $J = (u + v)$, $L = (u, v)$.
b) Stabilire se esistono $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$ tali che $w = \alpha_1 u + \alpha_2 v$.
c) Determinare un campo infinito che contiene $K = \mathbb{Z}[i]/L$ come sottocampo.

Università di Bologna C.d.L. in Matematica A.A. 2007–08

Prova scritta di Algebra II (M. Manaresi) – 18.06.08

Giustificare sempre le risposte!

Gli studenti di **ALGEBRA COMPUTAZIONALE I** debbono svolgere il primo esercizio e il secondo esercizio.

Esercizio 1. Sia $\mathbb{Z}_{18}{}^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{18}$, siano S_3 e S_6 i gruppi delle permutazioni su 3 e 6 lettere rispettivamente.

a) Stabilire se esiste un omomorfismo suriettivo dal gruppo $\mathbb{Z}_{18}{}^*$ al gruppo S_3.
b) Individuare (nel caso esistano) tutti i possibili omomorfismi di gruppi iniettivi e tutti i possibili omomorfismi di gruppi suriettivi $\mathbb{Z}_{18}{}^* \to S_6$.
c) Stabilire se esiste un omomorfismo di gruppi $S_6 \to \mathbb{Z}_{18}{}^*$ il cui nucleo sia il sottogruppo H di S_6 generato dalle permutazioni $\alpha = (13)(24)$ e $\beta = (12)(34)$.

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, siano $I := (x^3 + 3x + 5, x+2)$, $J_1 := (x-1, 3)$ e $J_2 := (x^2+3x+2)$ tre suoi ideali, sia $A := \mathbb{Z}[x]/I$ l'anello quoziente, $\pi : \mathbb{Z}[x] \to A$ la proiezione canonica.

a) Si determini un divisore di zero dell'anello A.
b) Si stabilisca se $\pi(J_1) = \pi(J_2)$.
c) Si determinino il nucleo e l'immagine dell'omomorfismo di anelli $\phi : \mathbb{Z}[x] \to \mathbb{Z}_9$ definito da $\phi(f(x)) = [f(-2)]_9$ per ogni $f \in \mathbb{Z}[x]$.
d) Si determini il numero degli elementi invertibili dell'anello A.

Esercizio 3. Siano $\mathbb{Q}$ e $\mathbb{C}$ i campi dei numeri razionali e dei numeri complessi, sia $u \in \mathbb{C}$ un numero algebrico il cui polinomio minimo su $\mathbb{Q}$ é il polinomio $p_u = x^6 + 3x^5 + 6x^4 + 7x^3 + 2x^2 - x + 1$ e sia $v = u^2 + u$.

a) Provare che v é radice del polinomio $f = x^3 + 3x^2 - x + 1 \in \mathbb{Q}[x]$.
b) Stabilire se f é il polinomio minimo di v su $\mathbb{Q}$.
c) Calcolare $[\mathbb{Q}(u) : \mathbb{Q}(v)]$.
d) Stabilire se esiste $z \in \mathbb{Q}(v)$ tale che $z \notin \mathbb{Q}$, ma $z^2 \in \mathbb{Q}$.

Esercizio 4. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss, siano $u = 120 + 234i$, $v = 23 - 58i$, $w = 27 + 6i$ tre suoi elementi e sia $I = (u, v)$ l'ideale generato da u, v.

a) Determinare $MCD(u, v)$.
b) Stabilire se l'ideale I é massimale e se $w \in I$.
c) Stabilire se esiste un un campo infinito K per il quale é definito un omomorfismo di anelli $\phi : \mathbb{Z}[i] \to K$ tale che $\ker \phi = I$.

Università di Bologna **C.d.L. in Matematica A.A. 2007–08**

Prova scritta di Algebra II (M. Manaresi) – 15.07.08

Giustificare sempre le risposte!

Esercizio 1. Si consideri il gruppo $G := S_3 \times \mathbb{Z}_4$ prodotto diretto del gruppo delle permutazioni su 3 lettere e del gruppo delle classi di resto modulo 4 e il suo sottogruppo $H :=< (123) > \times < [2]_4 >$.

a) Si stabilisca se in G i due elementi $\alpha = ((123), [2]_4)$ e $\beta = ((132), [3]_4)$ sono coniugati.

b) Si scrivano eplicitamente gli elementi dei due laterali $((12), [3]_4)H$ e $((13), [3]_4)H$, stabilendo se coincidono.

c) Si provi che H é un sottogruppo normale di G e si scriva un omomorfismo suriettivo $\phi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ tale che $Ker\,\phi = H$.

d) FACOLTATIVO Si stabilisca se G ha un sottogruppo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, ossia se esiste un omomorfismo di gruppi iniettivo $\psi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$.

Esercizio 2. Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, sia I un suo ideale contenente i due polinomi x^2 e $3x$.

a) Si determini l'ideale I in modo che l'anello $\mathbb{Z}[x]/I$ sia un campo.

b) É possibile determinare I in modo che l'anello $\mathbb{Z}[x]/I$ sia isomorfo a $\mathbb{Z}_6$?

c) Se l'anello $\mathbb{Z}[x]/I$ é un campo, é necessariamente un campo finito?

Esercizio 3. Sia $\mathbb{Q}$ il campo dei numeri razionali, sia u il numero reale $\sqrt{3+\sqrt{3}}$ e p_u il suo polinomio minimo su $\mathbb{Q}$.

a) Si scriva una base di $\mathbb{Q}(u)$ come $\mathbb{Q}$-spazio vettoriale.

b) Si stabilisca se $\sqrt{6}$ appartiene a $\mathbb{Q}(u)$.

c) Si determini il campo di spezzamento L di p_u su $\mathbb{Q}$.

Esercizio 4. Sia $p(x) = x^3 - x^2 + 1 \in \mathbb{Z}_2[x]$ e sia $L = \mathbb{Z}_2[x]/(p(x))$.

a) Si provi che L é un campo, se ne calcoli la caratteristica e si scrivano tutti i suoi elementi.

b) Si stabilisca se il polinomio p si spezza in fattori lineari su L e in caso affermativo si scriva la decomposizione.

c) Si stabilisca se su L si spezzano in fattori lineari i polinomi $f = x^3 + x + 1$ e $g = x^2 + x + 1$. In caso di risposta negativa si determini "il piú piccolo" campo K, estensione del campo $\mathbb{Z}_2$, su cui i polinomi p, f, g si spezzano in fattori lineari.

d) Si stabilisca se il campo K di cui al punto precedente e' un'estensione semplice di $\mathbb{Z}_2$ e se puo' essere contemporaneamente il campo di spezzamento di un polinomio di grado 5 e di un polinomio di grado 6.

Università di Bologna C.d.L. in Matematica A.A. 2007–08

Prova scritta di Algebra II (M. Manaresi) – 18.09.08

Giustificare sempre le risposte!

Esercizio 1.

Siano $\mathbb{Z}$ e $\mathbb{Z}_{24}$ i gruppi rispettivamente degli interi e delle classi di resto modulo 24; sia G il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{14}$ delle classi di resto modulo 14.

a) Elencare i morfismi da G a $\mathbb{Z}_{24}$.

b) Trovare un morfismo $\phi : \mathbb{Z}_{24} \to G$ tale che $\ker \phi = \langle [3]_{24} \rangle$.

c) Esiste un morfismo suriettivo da $\mathbb{Z}$ a $G \times \mathbb{Z}_{24}$?

Esercizio 2.

Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, sia $I = (x^2 - 3x + 2)$ un suo ideale; sia $\mathbb{Z}[x]/I$ l'anello quoziente e $\pi : \mathbb{Z}[x] \to \mathbb{Z}[x]/I$ la proiezione canonica. Siano $L = (x - 1)$ e $M = (x - 2)$ due ideali di $\mathbb{Z}[x]$ e siano $\bar{L} = \pi(L)$ e $\bar{M} = \pi(M)$ le loro immagini nell'anello quoziente $\mathbb{Z}[x]/I$.

a) Si determinino tutti gli ideali J di $\mathbb{Z}[x]$ per i quali l'applicazione $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ che a ogni elemento $[f]_I \in \mathbb{Z}[x]/I$ associa l'elemento $[f]_J \in \mathbb{Z}[x]/J$ é ben definita ed é un omomorfismo di anelli.

b) Tra gli ideali J di cui al punto a) ne esistono alcuni per cui l'anello $\mathbb{Z}[x]/J$ é un campo?

c) Si determini un ideale proprio N di $\mathbb{Z}[x]$, $N \neq L$, tale che $\pi(N) = \pi(L)$.

d) Tra gli ideali $\bar{L}$ e $\bar{M}$ esiste una relazione di inclusione?

Esercizio 3.

Sia $\mathbb{Q}$ il campo dei numeri reali, sia $\mathbb{R}$ il campo dei numeri razionali, siano $u, v \in \mathbb{R} - \mathbb{Q}$ e si denotino con $\sigma_u : \mathbb{Q}[x] \to \mathbb{R}$ e con $\sigma_v : \mathbb{Q}[x] \to \mathbb{R}$ i rispettivi morfismi sostituzione.

a) Se $\ker \sigma_u \neq \ker \sigma_v$, posso concludere che $\mathbb{Q}(u)$ non é isomorfo a $\mathbb{Q}(v)$?

b) Se $\mathbb{Q}(u) \subset \mathbb{Q}(v)$, posso concludere che $\ker \sigma_v \subset \ker \sigma_u$?

c) Sia scelga $u = \sqrt{\sqrt{2} - 1}$ e si determini v in modo che $\ker \sigma_u \cap \ker \sigma_v = (0)$.

Esercizio 4. Sia $p(x) = x^6 + x^4 - x^3 + x^2 - x + 1 \in \mathbb{Z}_3[x]$ e siano $p_1, \ldots, p_r$ i polinomi irriducibili di $\mathbb{Z}_3[x]$ che dividono p.

a) Si determinino $p_1, \ldots, p_r$ e la decomposizione di p in irriducibili di $\mathbb{Z}_3[x]$.

b) Per ognuno dei campi $K_i = \mathbb{Z}_3[x]/(p_i)$ si calcoli la caratteristica e si scrivano tutti gli elementi.

c) Si stabilisca se tra i campi $K_i = \mathbb{Z}_3[x]/(p_i)$ ne esiste almeno uno su cui il polinomio p si spezza in fattori lineari e in caso affermativo si scriva la decomposizione.

d) Si determini il campo di spezzamento L del polinomio p su $\mathbb{Z}_3[x]$ e si stabilisca se tale campo é un'estensione semplice di $\mathbb{Z}_3$.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Esercitazione scritta di Algebra II (M. Manaresi) – 19.12.08

Giustificare sempre le risposte!

Esercizio 1.

Siano $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ il gruppo prodotto diretto dei gruppi delle classi di resto modulo 2 e 4 rispettivamente, S_6 il gruppo delle permutazioni su 6 lettere. Si considerino le seguenti applicazioni da G a S_6:

$$f_1(([a]_2, [b]_4)) = (12)^a(34)^b,$$

$$f_2(([a]_2, [b]_4)) = (12)^a(345)^b,$$

$$f_3(([a]_2, [b]_4)) = (12)^a(3456)^b,$$

$$f_4(([a]_2, [b]_4)) = (12)^a(2345)^b,$$

$$f_5(([a]_2, [b]_4)) = (123)^a(456)^b.$$

a) Si stabilisca quali delle applicazioni $f_1, \ldots, f_5$ é un omomorfismo di gruppi e nei casi casi in cui f_i é un omomorfismo si determinino $\ker f_i$ e Imf_i.

b) Nei casi in cui f_i é un omomorfismo si stabilisca se Imf_i é un sottogruppo normale di S_6.

c) Si stabilisca se esiste un sottogruppo normale di S_6 con 6 elementi.

Esercizio 2.

Sia $\mathbb{Z}[x]$ l'anello dei polinomi a coefficienti interi, siano $I = (x^2+3x-9, x-3)$, $J = (x^3, 27)$ due suoi ideali.

a) Si stabilisca se é vero che tutti i polinomi che stanno in I hanno il termine noto divisibile per 3.

b) Si provi che $[x-2]_I$ é un divisore dello zero non nullo dell'anello quoziente $\mathbb{Z}[x]/I$.

c) Si stabilisca se l'applicazione $\phi : \mathbb{Z}[x]/J \to \mathbb{Z}[x]/I$ che a ogni elemento $[f]_J \in \mathbb{Z}[x]/J$ associa l'elemento $[f]_I \in \mathbb{Z}[x]/I$ é ben definita ed é un omomorfismo di anelli.

Esercizio 3.

Sia $\mathbb{Q}$ e $\mathbb{R}$ i campi dei numeri razionali e dei numeri reali rispettivamente, siano $f = x^4 - 8x^2 + 9$, $g = (x^2 - 7)(x^4 - 8x^2 + 9) \in \mathbb{Q}[x]$ e sia $u \in \mathbb{R}$ una radice reale del polinomio f.

a) Si stabilisca se nel campo $\mathbb{Q}(u)$ l'elemento $\frac{u-1}{u+2}$ puó essere rappresentato da un polinomio in u e in caso affermativo si determini tale polinomio.

b) Si determinino i campi di spezzamento K e L rispettivamente di f e g su $\mathbb{Q}$, calcolandone la dimensione come $\mathbb{Q}$-spazi vettoriali e stabilendo se sono estensioni semplici di $\mathbb{Q}$.

Esercizio 4.

Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani, siano $u = 19 + 8i$, $v = (14 - a) + i(14 + a)$ con $a \in \mathbb{Z}$ due suoi elementi e sia $I = (u, v)$ l'ideale di $\mathbb{Z}[i]$ da essi generato.

a) Si determinino i valori di $a \in \mathbb{Z}$ per i quali l'anello quoziente $\mathbb{Z}[i]/I$ é un campo.

b) Per $a = 3$ si determini la caratteristica e il numero degli elementi del campo $K := \mathbb{Z}[i]/I$.

c) Si scriva un polinomio irriducibile di grado 3 a coefficienti in K e un'estensione di K su cui tale polinomio si spezza in fattori lineari.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 8.1.09

Giustificare sempre le risposte!

Esercizio 1.

Sia G il gruppo degli elementi invertibili dell'anello $\mathbb{Z}[x] \times \mathbb{Z}_8$ prodotto diretto dell'anello dei polinomi a coefficienti interi e dell'anello delle classi di resto modulo 8, sia S_6 il gruppo delle permutazioni su 6 lettere.

a) Si scriva un omomorfismo di gruppi iniettivo $f : G \to S_6$. nell'anello quoziente $\mathbb{Z}_3[x]/I$.

b) Si stabilisca se esiste un omomorfismo di gruppi $g : G \to S_6$ tale che $Im\, g = \{id, (12), (34), (12)(34)\}$ e in caso affermativo si determini $\ker g$.

c) Per ognuna delle seguenti coppie di sottogruppi G_i, H_i di S_6 si stabilisca se essi sono coniugati in S_6, ossia se esiste $\alpha_i \in S_6$ tale che $C_{\alpha_i}(G_i) = H_i$, dove C_{α_i} indica il coniugio rispetto ad α_i, e in caso positivo si determini α_i:

$$G_1 =< (123456) >, \quad H_1 =< (12), (345) >;$$

$$G_2 = \{\gamma \in S_6 \,|\, \gamma(4) = 4, \gamma(5) = 5, \gamma(6) = 6\}, \quad H_2 =< (12), (345) >;$$

$$G_3 =< (12), (45) >, \quad H_3 =< (13), (24) > .$$

Esercizio 2.

Sia $\mathbb{Z}_3[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_3$ delle classi di resto modulo 3, siano $a(x) = x^4 - x^2 + 2x - 2$, $b(x) = x^3 - x^2 + x + 2 \in \mathbb{Z}_3[x]$; siano $I = (a(x))$, $J = (a(x), b(x))$ due ideali dell'anello $\mathbb{Z}_3[x]$. Sia $\mathbb{Z}[i]$ l'anello degli interi gaussiani.

i) Si determinino tutti gli ideali dell'anello quoziente $\mathbb{Z}_3[x]/I$.

ii) Si provi che nell'anello quoziente $\mathbb{Z}_3[x]/I$ l'elemento $[b(x)]_I$ é uno zero-divisore.

iii) Si stabilisca se gli ideali $S_1 = (x^3 + x^2 - x - 1), S_2 = (x^2 + 2)$ hanno la stessa immagine nell'anello quoziente $\mathbb{Z}_3[x]/I$.

iv) Si mostri che esiste un omomorfismo di anelli dall'anello $\mathbb{Z}[x]/J$ al campo $\mathbb{Z}[i]/(3)$ e si stabilisca se tale omomorfismo é iniettivo, suriettivo, un isomorfismo.

v) Si determini un generatore del gruppo moltiplicativo del campo $\mathbb{Z}[i]/(3)$.

vi) Si determini il piú piccolo campo K estensione del campo $\mathbb{Z}_3$ su cui i polinomi $a(x)$ e $b(x)$ si spezzano in fattori lineari e si calcoli $[K : \mathbb{Z}_3]$.

Esercizio 3.

Siano $\mathbb{Q}$ e $\mathbb{R}$ i campi dei numeri razionali e dei numeri reali rispettivamente, sia $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$, sia $u \in \mathbb{R}$ una radice reale del polinomio f e sia L il campo di spezzamento di f su $\mathbb{Q}$. Sia $g = x^2 + 2 \in \mathbb{Q}[x]$.

a) Si provi che anche $v = u^2 - 2$ é radice di f e si determini la terza radice w del polinomio.

b) Si stabilisca se esiste un polinomio di grado 1 in u che rappresenta la funzione razionale $\frac{1}{u^2} \in \mathbb{Q}(u)$.

c) Si stabilisca se L é un'estensione semplice di $\mathbb{Q}$ e si calcoli $[L : \mathbb{Q}]$.

d) Si determini il campo di spezzamento M del polinomio fg su $\mathbb{Q}$, si calcoli $[M : \mathbb{Q}]$ e si stabilisca se $L = M$.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 12.2.09

Giustificare sempre le risposte!

Esercizio 1.

Sia G il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_6$ prodotto diretto degli anelli delle classi di resto modulo 2 e 6 rispettivamente. Siano S_6 il gruppo delle permutazioni su 6 lettere, H il sottogruppo di S_6 costituito dalle permutazioni pari, S_6/H il gruppo quoziente.

a) Si stabilisca se esiste un omomorfismo di gruppi iniettivo $f : G \to S_6$.

b) Si stabilisca se esiste un omomorfismo di gruppi $g : G \to S_6$ tale che $Im\, g = < (12), (345) >$ e in caso affermativo si determini $\ker g$.

c) Si provi che H é un sottogruppo normale di S_6 , si scriva un omomorfismo di gruppi suriettivo $h : G \to S_6/H$ e si calcoli $\ker h$.

Esercizio 2. Sia $\mathbb{Z}_5[x]$ l'anello dei polinomi a coefficienti nel campo $\mathbb{Z}_5$ siano $f = x^4 + [2]_5x^3 + [3]_5x^2 + [4]_5x + [2]_5$, $g = x^4 + x^3 + [3]_5x^2 + [2]_5x + [2]_5$ due suoi elementi e siano $I = (f), J = (g)$ gli ideali di $\mathbb{Z}_5[x]$ generati rispettivamente dai polinomi f e g .

a) Stabilire se l'elemento $[x + 2]_I$ dell'anello $A := \mathbb{Z}_5[x]/I$ ammette inverso in Λ e in caso positivo determinarlo.

b) Determinare un generatore degli ideali $I + J$ e $I \cap J$, stabilendo sono primi e se sono massimali. Nel caso gli ideali non siano massimali, si determini, per ognuno di essi, un ideale massimale che lo contiene.

c) Nel caso l'anello $\mathbb{Z}_5[x]/(I + J)$ sia un campo, si determini un generatore del suo gruppo moltiplicativo.

d) Si stabilisca se i campi di spezzamento L_1 e L_2 dei polinomi f e g sul campo $\mathbb{Z}_5$ sono tra loro isomorfi e si calcoli $[L_i : \mathbb{Z}_5]\, (i = 1, 2)$.

e) Se $\mathbb{Z}[i]$ é l'anello degli interi gaussiani, si stabilisca se esistono isomorfismi di anelli tra L_1, $\mathbb{Z}[i]/(5)$ e $\mathbb{Z}[i]/(2 + i)$.

Esercizio 3.

Siano $\mathbb{Q}$ e $\mathbb{R}$ i campi dei numeri razionali e dei numeri reali rispettivamente, sia $f = x^4 - 12x^2 + 25 \in \mathbb{Q}[x]$ e sia $u \in \mathbb{R}$ una radice del polinomio f.

a) Si calcoli $[\mathbb{Q}(u) : \mathbb{Q}]$.

b) Si stabilisca se i numeri reali $\sqrt{11}$, $\sqrt[3]{11}$, π appartengono al campo $\mathbb{Q}(u)$.

c) Si stabilisca se $\frac{1}{u^2+2} = u^2 + 10$ in $\mathbb{Q}(u)$.

d) Si stabilisca se il campo di spezzamento L di f su $\mathbb{Q}$ é un'estensione semplice di $\mathbb{Q}$ e si calcoli $[L : \mathbb{Q}]$.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 4.06.09

Giustificare sempre le risposte!

Esercizio 1.

Sia $G := \mathbb{Z}_9{}^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_9$ delle classi di resto modulo 9.

a) Si stabilisca se G é ciclico e in caso positivo si determini un generatore.

b) Si stabilisca quanti sono gli omomorfismi di $G \to G$, indicando espressamente quanti di essi sono isomorfismi.

c) Si mostri che l'applicazione $\phi : G \to G$ definita da

$$\phi([1]_9) = \phi([8]_9) = [1]_9, \quad \phi([2]_9) = \phi([7]_9) = [7]_9, \quad \phi([4]_9) = \phi([5]_9) = [4]_9,$$

é un omomorfismo di gruppi e se ne calcoli nucleo e immagine.

Esercizio 2. Siano $K_1 = \mathbb{Z}_2[x]/(x^2+x+1)$, $K_2 = \mathbb{Z}_2[x]/(x^3+x+1)$, $K_3 = \mathbb{Z}_3[x]/(x^3+x+1)$, $K_4 = \mathbb{Z}_2[x]/(x^4+x+1)$, $K_5 = \mathbb{Z}_3[x]/(x^4+x+1)$.

a) Si stabilisca quali degli anelli K_i, $i = 1, \dots 5$, sono campi.

b) Si stabilisca se esistono omomorfismi iniettivi $K_1 \to K_2$, $K_1 \to K_4$, $K_2 \to K_4$.

Esercizio 3.

Siano $F \subset K \subset L$ estensioni di campi e sia $u \in L$.

a) Si provi che se u é algebrico su F allora lo é anche su K.

b) Si mostri che se u é algebrico su F (e dunque su K) il polinomio minimo di u su K divide il polinomio minimo di u su F in $F[x]$.

c) Si trovi un esempio in cui u é algebrico su K ma non su F.

Esercizio 4.

Siano $\mathbb{Z}[i]$ e $\mathbb{Z}_5$ l'anello degli interi di Gauss e il campo delle classi di resto modulo 5 rispettivamente e sia $\psi : \mathbb{Z}[i] \to \mathbb{Z}_5$ l'applicazione definita da $\psi(a+ib) = [a]_5 + 3[b]_5$.

a) Mostrare che ψ é un omomorfismo suriettivo e determinare un generatore di $\ker \psi$.

b) Indicata con $\pi : \mathbb{Z}[i] \to \mathbb{Z}[i]/\ker \psi$ la proiezione canonica sul quoziente, si stabilisca se i due ideali $(3-i)$ e (5) dell'anello $\mathbb{Z}[i]$ hanno la stessa immagine mediante π.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 23.06.09

Giustificare sempre le risposte!

Esercizio 1.

Siano $(\mathbb{C},+)$ e $(\mathbb{R},+)$ i gruppi additivi dei numeri complessi e dei numeri reali rispettivamente, sia $(\mathbb{C}^*,\cdot)$ il gruppo moltiplicativo dei numeri complessi non nulli. Sia $Re : (\mathbb{C},+) \to (\mathbb{R},+)$ l'applicazione che ad ogni numero complesso associa la sua parte reale, sia $\phi : (\mathbb{C}^*,\cdot) \to (\mathbb{C}^*,\cdot)$ l'applicazione di coniugio complesso (che ad ogni numero complesso $z = a + ib$ associa il suo coniugato $\bar{z} = a - ib$).

a) Si provi che l'applicazione Re é un omomorfismo di gruppi, se ne determini il nucleo N e l'immagine H e si definisca l'isomorfismo canonico $\mathbb{C}/N \to H$.

b) Si provi che l'omomorfismo di coniugio ϕ é un automorfismo del gruppo $(\mathbb{C}^*,\cdot)$.

c) Si verifichi che se ξ é una radice n-esima dell'unitá, allora $\bar{\xi}^k = \xi^{n-k}$ per ogni $0 \le k \le n-1$.

Esercizio 2.

Siano $\mathbb{Z}[i]$ l'anello degli interi di Gauss, siano $A := \mathbb{Z}[i]/(30+10i)$, $B := \mathbb{Z}[i]/(7+6i, 3+5i)$ due suoi anelli quoziente.

a) Si scrivano tutti gli ideali primi e tutti gli ideali massimali degli anelli A e B.

b) Si stabilisca se esiste un omomorfismo di anelli iniettivo $A \to B$.

Esercizio 3.

Sia $\mathbb{Q}$ il campo dei numeri razionali e sia $u = \sqrt[4]{3}$

a) Si provi che u é algebrico e si determini il suo polinomio minimo p_u.

b) Si determini il campo di spezzamento L di p_u su $\mathbb{Q}$ e si calcoli $[L : \mathbb{Q}]$.

c) Si stabilisca se il campo $\mathbb{Q}(u)$ é isomorfo al campo $\mathbb{Q}(i\sqrt[4]{3})$.

d) Si razionalizzi l'espressione $\frac{1}{u^3-u}$.

Esercizio 4. Siano K un campo e siano E_q e F_r due sottocampi finiti di K di ordini q ed r rispettivamente.

a) Si stabilisca se i campi K, E_q e F_r possono avere caratteristiche diverse.

b) Si studi $E_q \cap F_r$ stabilendo se é un campo e calcolandone la caratteristica e l'ordine.

c) Si stabilisca sotto quali condizioni esiste un omomorfismo iniettivo $E_q \to F_r$.

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 16.07.09

Giustificare sempre le risposte!

Esercizio 1.

Sia $\mathbb{Z}_{12}$ l'anello delle classi di resto modulo 12 e sia $\mathbb{Z}_{12}^*$ il gruppo moltiplicativo degli elementi invertibili dell'anello $\mathbb{Z}_{12}$.

a) Si determinino i generatori, i sottogruppi e i gruppi quoziente del gruppo $(\mathbb{Z}_{12}, +)$.

b) Si scriva un omomorfismo di gruppi non nullo $\psi : (\mathbb{Z}_{12}, +) \to (\mathbb{Z}_{28}, +)$, se ne determini il nucleo N e l'immagine H.

c) Si scriva l'isomorfismo di gruppi canonico $\phi : \mathbb{Z}_{12}/N \to H$.

d) Al punto b) é possibile scegliere l'omomorfismo ψ in modo tale che il gruppo immagine H sia isomorfo al gruppo moltiplicativo $(\mathbb{Z}_{12}^*, \cdot)$?

Esercizio 2.

Siano $\mathbb{Z}[i]$ l'anello degli interi di Gauss, siano $\alpha := 9+2i$, $\beta := 15+9i$ due suoi elementi.

a) Si determini un massimo comun divisore tra α e β e un'identitá di Bezout per esso.

b) Si determini un generatore degli ideali $(\alpha)+(\beta)$ e $(\alpha)\cap(\beta)$ di $\mathbb{Z}[i]$.

c) Si stabilisca se l'immagine dell'ideale (β) nell'anello $\mathbb{Z}[i]/(\alpha)$ é un ideale proprio.

Esercizio 3.

Sia $\xi \in \mathbb{C}$ (campo dei numeri complessi) una radice primitiva ottava dell'unitá.

a) Si determini il polinomio minimo p_ξ di ξ su $\mathbb{Q}$ (campo dei numeri razionali).

b) Si determini una base di $\mathbb{Q}(\xi)$ su $\mathbb{Q}$ e si scriva il generico elemento di $\mathbb{Q}(\xi)$.

c) Si stabilisca se il polinomio p_ξ si spezza in fattori lineari sul campo $\mathbb{Q}(\xi)$.

d) Si razionalizzi l'espressione $\frac{1}{\xi^2}$.

Esercizio 4.

Sia K un campo e sia $K(x)$ il campo delle funzioni razionali in una variabile su K.

Si provi che ogni $u \in K(x) - K$ é trascendente su K .

Università di Bologna **C.d.L. in Matematica A.A. 2008–09**

Prova scritta di Algebra II (M. Manaresi) – 17.09.09

Giustificare sempre le risposte!

Esercizio 1.

Sia $G := \mathbb{Z}_2 \times \mathbb{Z}_4$ il gruppo prodotto diretto dei gruppi additivi delle classi di resti modulo 2 e 4 rispettivamente, sia S_n il gruppo delle permutazioni su n lettere.

a) Si stabilisca se per ogni intero $n \geq 2$ esiste un omomorfismo di gruppi non banale $\phi : G \to S_n$.

b) Si stabilisca per quali interi $n \geq 2$ esiste un omomorfismo di gruppi iniettivo $\psi : G \to S_n$ e lo si determini.

c) Posto $n = 8$, si stabilisca se esiste un sottogruppo normale H di S_8 isomorfo a G.

d) Posto $n = 8$, si determinino due diversi sottogruppi H_1 e H_2 di S_8 isomorfi a G e tra loro coniugati, esplicitando l'omomorfismo di coniugio da cui sono legati.

Esercizio 2.

Sia $\mathbb{Z}_3$ il campo delle classi di resto modulo 3 e sia $f(x) = 2x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$, sia $A = \mathbb{Z}_3[x]/(f(x))$ l'anello quoziente e $\pi : \mathbb{Z}_3[x] \to A$ la proiezione canonica sul quoziente.

a) Si stabilisca se A é un dominio di integritá.

b) Si mostri che l'elemento $x^3 + (f) \in A$ é invertibile e se ne trovi l'inverso.

c) Si stabilisca per quali $a \in \mathbb{Z}$ l'immagine mediante π dell' ideale $I = (x^2+ax-1) \subset \mathbb{Z}_3[x]$ é un ideale proprio dell'anello quoziente A.

d) Si stabilisca se esiste un campo $K \neq \mathbb{Z}_3$ per il quale si puó definire un omomorfismo di anelli suriettivo $A \to K$.

e) Se per un campo L si puo' definire un omomorfismo di anelli suriettivo $A \to L$, che cosa si puó dire della catteristica di L?

Esercizio 3.

Sia $f(x) = x^5 - 3x^4 - 10x^3 + 30x^2 + 14x - 42 \in \mathbb{Z}[x]$.

a) Si determinino le radici razionali del polinomio f e si decomponga il polinomio in irriducibili di $\mathbb{Z}[x]$ e di $\mathbb{R}[x]$.

b) Si determini il campo di spezzamento E di f su $\mathbb{Q}$, stabilendo se é un'estensione semplice di $\mathbb{Q}$ e si calcoli $[E : \mathbb{Q}]$.

c) Si stabilisca se esiste un campo L tale che $\mathbb{Q} \subset L \subset E$ e $[E : L] = [L : Q]$.

Esercizio 4.

Si consideri l'anello $A = \mathbb{Z}[\sqrt{-5}]$ e i suoi elementi

$$a = 6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5}), \qquad b = 2 \cdot (1 + \sqrt{-5}).$$

Si provi che in A non esiste un massimo comun divisore di a e b.

[*Suggerimento*: si supponga per assurdo che esista un massimo comun divisore d e si studi la sua norma.]