CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
18 MAGGIO 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Sia $S = \mathbb{N} \setminus \{0, 1\}$. Per ogni $k \in \mathbb{N}^{\#}$ si ponga $S_k = \{n \in S \mid n \text{ è diviso da esattamente } k \text{ primi positivi distinti}\}$ (ad esempio, $8 \in S_1$, $500 \in S_2$).

(*i*) Verificare che $\mathcal{F} := \{S_k \mid k \in \mathbb{N}^{\#}\}$ è una partizione di S.
(*ii*) Esiste una relazione di equivalenza $\mathcal{R}$ in S tale che $\mathcal{F} = S/\mathcal{R}$?
(*iii*) In caso affermativo, descrivere la classe di equivalenza di 210 rispetto a tale relazione $\mathcal{R}$.

Esercizio 2. Sia $f\colon n \in \mathbb{N} \longmapsto \pi(n) \in \mathcal{P}(\mathbb{P})$ (come di consueto, $\mathbb{P}$ indica l'insieme dei numeri primi positivi e, per ogni $n \in \mathbb{N}$, $\pi(n) = \{p \in \mathbb{P} : p \mid n\}$). Si consideri la relazione d'ordine σ_f definita in $\mathbb{N}$ da:

$$(\forall\, a, b \in \mathbb{N})\,(a\ \sigma_f\ b \iff a = b \ \vee\ f(a) \subset f(b))\,.$$

(*i*) Individuare gli eventuali minimo, massimo, elementi minimali, elementi massimali in $(\mathbb{N}, \sigma_f)$. $(\mathbb{N}, \sigma_f)$ è un reticolo?
(*ii*) Se possibile, determinare un sottoinsieme Y di $\mathbb{N}$ tale che $|Y| = 4$ e (Y, σ_f) sia un reticolo, specificando se esso è un reticolo booleano.
(*iii*) Posto $X = \{15, 21, 105, 210, 315\}$, descrivere (se esistono) in $(\mathbb{N}, \sigma_f)$: i minoranti di X, i maggioranti di X, $\inf X$, $\sup X$. Si disegni il diagramma di Hasse di (X, σ_f).

Esercizio 3. Si studi l'operazione $*$ definita sull'insieme $R = \mathbb{Z}_{40}$ delle classi di resto modulo 40 ponendo, per ogni a, $b \in R$,

$$a * b = a + \overline{25}b - \overline{10}.$$

In particolare, si stabilisca se $*$ è commutativa e se è associativa, se esistono in $(R, *)$ elementi neutri a destra, elementi neutri a sinistra, elementi neutri. L'operazione $*$ è distributiva a destra rispetto alla ordinaria addizione in $\mathbb{Z}_{40}$?

Esercizio 4. Si enunci il teorema di Ruffini generalizzato.

Dati i polinomi $h = (x^2 - 1)(3x + 2)$ e $k = (x - 4)^2$ in $\mathbb{Q}[x]$,

(*i*) esiste un polinomio $g \in \mathbb{Q}[x]$ tale che $f = h + gk$ abbia 1 e -1 come radici? Nel caso, fornirne un esempio e rispondere alle domande che seguono:
(*ii*) è possibile scegliere un tale g in modo che f abbia grado 3?
(*iii*) è possibile scegliere un tale g in modo che f abbia grado 10?
(*iv*) esistono infiniti $g \in \mathbb{Q}[x]$ con la proprietà richiesta in (*i*)?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
6 SETTEMBRE 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Si studi l'operazione $*$ definita in $\mathbb{Z}_{10}$ da

$$a * b = \bar{3}ab - a - b + \bar{4}$$

per ogni $a, b \in \mathbb{Z}_{10}$, stabilendo:

(*i*) se $*$ è commutativa;
(*ii*) se $*$ è associativa;
(*iii*) se $*$ ammette elemento neutro;
(*iv*) quali tra $\bar{0}$, $\bar{1}$, $\bar{2}$ e $\bar{6}$ sono invertibili in $(\mathbb{Z}_{10}, *)$, determinando gli eventuali inversi;
(*v*) che genere di struttura è $(\mathbb{Z}_{10}, *)$.

Esercizio 2. Sia σ la relazione d'ordine definita in $\mathbb{N} \times \mathbb{N}$ da:

$$(\forall\, a, b, c, d \in \mathbb{N})\,((a, b)\ \sigma\ (c, d) \iff a + 1 \mid c + 1 \ \wedge\ b \leq d)\,.$$

(*i*) Individuare gli eventuali minimo, massimo, elementi minimali, elementi massimali in $(\mathbb{N}\times\mathbb{N}, \sigma)$.
(*ii*) Determinare i maggioranti di $X := \{0, 1, 2, 3\} \times \{7\}$ in $(\mathbb{N} \times \mathbb{N}, \sigma)$ e, se esiste, $\sup X$ (sempre in $(\mathbb{N} \times \mathbb{N}, \sigma)$).
(*iii*) Posto $S = \{(0, 0), (1, 1), (3, 3), (3, 7), (5, 5), (11, 1), (11, 11), (119, 11)\}$, si disegni il diagramma di Hasse di (S, σ). (S, σ) è un reticolo? È un reticolo booleano? È un reticolo complementato? È un reticolo distributivo?

Esercizio 3. Data una relazione di equivalenza α su un insieme K, cosa è, per definizione, la classe di equivalenza rispetto ad α di un elemento $t \in K$? E cosa è l'insieme quoziente K/α?

Sia ora $\sim$ la relazione binaria definita in $J := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ponendo

$$a \sim b \iff a^2 - 1 \equiv_8 b^2 - 1$$

per ogni $a, b \in J$. Dopo aver verificato che $\sim$ è una relazione di equivalenza,

(*i*) si descrivano esplicitamente $[2]_\sim$ e $[9]_\sim$.
(*ii*) Quanti e quali sono gli elementi di $J/\sim$?
(*iii*) Descrivere, se possibile, un sottoinsieme A di J tale che, $|A| = 6$ e, rispetto alla relazione di equivalenza indotto su esso da $\sim$, A abbia esattamente due classi.

Infine, si consideri la relazione di equivalenza τ definita in $\mathbb{Z}$ ponendo $a\ \tau\ b \iff a^2 - 1 \equiv_8 b^2 - 1$ per ogni $a, b \in \mathbb{Z}$.

(*iv*) Quanti elementi ha $\mathbb{Z}/\tau$?

Esercizio 4. Determinare gli interi n tali che il polinomio $f := \bar{3}x^5+\bar{2}x^4+\bar{5}x^3+\bar{6}\bar{n}x^2-\bar{4}x+\bar{1} \in \mathbb{Z}_{31}[x]$ sia divisibile (in $\mathbb{Z}_{31}[x]$) per $x - \bar{2}$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
19 OTTOBRE 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Assegnati numeri interi a, b, d, r, si dica cosa significano, per definizione, le frasi:

(i) a è divisore di b;
(ii) a è multiplo di b;
(iii) d è un massimo comun divisore tra a e b;
(iv) r è il resto della divisione di a per b. In quest'ultimo caso, è necessario premettere una condizione su b, quale?

Esercizio 2. Si studino iniettività e suriettività dell'applicazione

$$\varphi\colon (a,b) \in \mathbb{N}\times\mathbb{N} \longmapsto 2^a 3^b \in \mathbb{N}^{\#}.$$

Detto $\mathcal{R}_\varphi$ il nucleo di equivalenza di φ, per ogni $(a,b)\in\mathbb{N}\times\mathbb{N}$ si determini $[(a,b)]_{\mathcal{R}_\varphi}$.

Si verifichi che la relazione binaria Σ così definita in $\mathbb{N}^{\#}\times\mathbb{N}^{\#}$:

$$\big(\forall (a,b),(c,d)\in\mathbb{N}^{\#}\times\mathbb{N}^{\#}\big)\big((a,b)\ \Sigma\ (c,d) \iff 2^a3^b \leq 2^c3^d\big)$$

è una relazione d'ordine. Σ è totale? $(\mathbb{N}^{\#}\times\mathbb{N}^{\#},\Sigma)$ è un reticolo? Nel caso lo sia, è distributivo?, è complementato?

Dire se le seguenti affermazioni sono vere o false (giustificando la risposta):

(1) $(\forall (a,b),(c,d)\in\mathbb{N}^{\#}\times\mathbb{N}^{\#})\ \big((a,b)\ \Sigma\ (c,d)\Rightarrow (a\leq c\ \wedge\ b\leq d)\big)$
(2) $(\forall (a,b),(c,d)\in\mathbb{N}^{\#}\times\mathbb{N}^{\#})\ \big((a\leq c\ \wedge\ b\leq d)\Rightarrow (a,b)\ \Sigma\ (c,d)\big)$

Esercizio 3. Si consideri il sottoinsieme $A=\{ax^3+bx^2+cx+d \mid a,b,c,d\in\mathbb{Z}_3\}$ di $\mathbb{Z}_3[x]$ e, per ogni $f=ax^3+bx^2+cx+d\in A$, si ponga $f'=\bar{3}ax^2+\bar{2}bx+c$. Caratterizzare i polinomi che costituiscono

$$B=\{f\in A \mid f'=0\}$$

in termini dei loro coefficienti (ciò che si chiede è dunque determinare condizioni necessarie e sufficienti su a, b, c e d affinché un polinomio $f=ax^3+bx^2+cx+d\in A$ appartenga a B).

Quanti sono gli elementi di B? Determinare la forma dei polinomi $f\in B$ che sono:

(i) divisibili per x;
(ii) divisibili per $x-\bar{1}$;
(iii) divisibili per $x+\bar{1}$.

Tra i polinomi in B, quanti sono quelli invertibili in $\mathbb{Z}_3[x]$? E quanti quelli irriducibili?

Esercizio 4. Si studi l'operazione binaria $*$ definita in $\mathbb{Z}_6\times\mathbb{Z}_6$ ponendo, per ogni $a,b,c,d\in\mathbb{Z}_6$,

$$(a,b)*(c,d)=(ac,bc).$$

(i) Si stabilisca se $*$ è associativa, se è commutativa, se ammette elemento neutro.
(ii) Verificare se $T:=\mathbb{Z}_6\times\{\bar{0},\bar{3}\}$ è chiusa rispetto a $*$.
(iii) Utilizzando opportune equazioni congruenziali, determinare, se esiste, un elemento $(u,v)\in T$ tale che $(\bar{5},\bar{3})*(u,v)=(u,v)*(\bar{5},\bar{3})=(\bar{1},\bar{3})$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
16 NOVEMBRE 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Relativamente a polinomi a coefficienti in un campo K, dare le definizioni di polinomio invertibile (e caratterizzare i polinomi invertibili), di polinomio monico, di polinomio irriducibile, di polinomio nullo, di coppia di polinomi associati.

Stabilire per quali primi p il polinomio $f = \overline{99}x^3 + \overline{144}x^2 + \overline{15}x + \overline{6} \in \mathbb{Z}_p[x]$ è:

(i) di grado 3;
(ii) nullo;
(iii) monico.

Si indichi il minimo primo $p > 10$ per il quale f abbia grado 3. Fissato questo primo,

(iv) $\overline{1}$ è radice di f?
(v) $\overline{2}$ è radice di f?
(vi) Tenendo presente il fatto che f ha al più una radice, si decomponga f come prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.
(vii) qual è (se esiste) il polinomio monico di $\mathbb{Z}_p[x]$ associato a f?

Esercizio 2. Siano $\mathbb{P}$ l'insieme dei numeri primi positivi e $M = \{n \in \mathbb{N} \mid n \geq 2\}$. Si studino iniettività e suriettività di $f\colon (p, q) \in \mathbb{P} \times \mathbb{P} \mapsto p + q \in M$ e si calcolino l'immagine $\vec{f}(\{(3, 7), (2, 11)\})$ e le antiimmagini $\overleftarrow{f}(\{18\})$ e $\overleftarrow{f}(\{2\})$.

Esercizio 3. Ancora nell'insieme $\mathbb{P} \times \mathbb{P}$ si consideri la relazione d'ordine Σ definita ponendo, per ogni $(a, b), (c, d) \in \mathbb{P} \times \mathbb{P}$,

$$(a, b)\ \Sigma\ (c, d) \iff \big((a \leq c) \wedge (b \leq d)\big).$$

(i) $(\mathbb{P} \times \mathbb{P}, \Sigma)$ è totalmente ordinato? Ha minimo? Ha massimo?
(ii) Determinare, in $(\mathbb{P} \times \mathbb{P}, \Sigma)$ gli insiemi dei minoranti e dei maggioranti di $A = \{(7, 5), (2, 11)\}$, e determinare, se esistono, $\inf A$ e $\sup A$.
(iii) Sia $X = \{(2, 3), (2, 5), (3, 5), (3, 7), (7, 11)\}$. Si disegni il diagramma di Hasse di (X, Σ). (X, Σ) è un reticolo? Se lo è, è distributivo? È complementato?

Esercizio 4. Siano $S = \{n \in \mathbb{N} \mid n \leq 6\}$ e $T = \{n \in \mathbb{Z} \mid (|n| < 10) \wedge (n \text{ è pari})\}$. Si indichino:

(i) $|S|$, $|T|$, $|S \cup T|$, $|S \cap T|$;
(ii) il numero delle applicazioni iniettive da S a T e quello delle applicazioni iniettive da T a S;
(iii) il numero delle parti di T che abbiano cardinalità 3;
(iv) il numero degli elementi di $\mathcal{P}(S) \cap \mathcal{P}(T)$; come possono essere caratterizzati questi elementi?

Infine, sapendo che esistono esattamente 877 partizioni dell'insieme S, quante sono le relazioni di equivalenza in S?

Esercizio 5. Si studi l'operazione binaria $\circ$ definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $X, Y \subseteq \mathbb{Z}$,

$$X \circ Y = (X \cap \mathbb{N}) \cup Y.$$

(i) Si stabilisca se $\circ$ è associativa, se è commutativa, se ammette elemento neutro.
(ii) $\mathcal{P}(\mathbb{Z} \setminus \mathbb{N})$ è chiusa rispetto a $\circ$? Se lo è, che tipo di struttura è $(\mathcal{P}(\mathbb{Z} \setminus \mathbb{N}), \circ)$? (un semigruppo, un monoide, un gruppo, nessuna di queste, ...; commutativa oppure no?)

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
14 DICEMBRE 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. L'applicazione $\psi\colon f \in \mathbb{Z}^{\mathbb{Z}} \mapsto f(2) \in \mathbb{Z}$ è iniettiva? È suriettiva?

Esercizio 2. Rappresentare con un diagramma di Venn: $\big((A \smallsetminus B) \cap (A \triangle C)\big) \cup (B \smallsetminus A)$.

Esercizio 3. In $A := \mathbb{Z} \times \mathbb{Z}_{10}$ si definisca un'operazione binaria $*$ ponendo, per ogni $a, c \in \mathbb{Z}$, $\bar{b}, \bar{d} \in \mathbb{Z}_{10}$,

$$(a, \bar{b}) * (c, \bar{d}) = (ac, \bar{b}\bar{d}\bar{a}).$$

(*i*) Si stabilisca se $*$ è associativa, se è commutativa, se ammette elementi neutri, a destra o a sinistra.
(*ii*) Posto $X = 1 + 10\mathbb{Z} = \{1 + 10k \mid k \in \mathbb{Z}\}$, $B := X \times \mathbb{Z}_{10}$ è chiusa rispetto a $*$? Se lo è, che tipo di struttura è $(B, *)$? (un semigruppo, un monoide, un gruppo, nessuna di queste, ...; commutativa oppure no?).

Si consideri la relazione binaria $\sim$ così definita in B: $\forall\, (a, \bar{b}), (c, \bar{d}) \in B$

$$(a, \bar{b}) \sim (c, \bar{d}) \iff (ac > 0 \wedge b \equiv_2 d).$$

(*iii*) $\sim$ è una relazione di equivalenza? Se lo è, rispondere anche alle domande che seguono.
(*iv*) Descrivere gli elementi di $[(131, \bar{4})]_{\sim}$. Questa classe è un insieme finito o infinito?
(*v*) Descrivere in modo esplicito l'insieme quoziente $B/\!\sim$. Quanti sono i suoi elementi?

Esercizio 4. Sia τ la relazione binaria definita in $\mathbb{N}$ ponendo, per ogni $n, m \in \mathbb{N}$,

$$m\ \tau\ n \iff \big((n \leq m) \wedge (\mathrm{rest}(n, 10) \leq \mathrm{rest}(m, 10)\big).$$

τ è una relazione d'ordine? Se lo è, si risponda alle domande che seguono.

(*i*) Si descrivano gli eventuali minimo, massimo, elementi minimali, elementi massimali in $(\mathbb{N}, \tau)$.
(*ii*) Posto $X = \{2, 6, 17, 23, 25, 32, 59, 105\}$, si disegni il diagramma di Hasse di (X, τ); si indichino gli eventuali minimo, massimo, elementi minimali, elementi massimali in (X, τ) e si stabilisca se (X, τ) è un reticolo.
(*iii*) Esiste $y \in X$ tale che $(X \smallsetminus \{y\}, \tau)$ sia un reticolo? Se sì, indicare un tale y.
(*iv*) In $(\mathbb{N}, \tau)$ determinare, se esistono, $\inf\{37, 54\}$ e $\sup\{37, 54\}$.
(*v*) $(\mathbb{N}, \tau)$ è un reticolo?

Esercizio 5. Sia $V = \{n \in \mathbb{N} \mid n < 10\}$ e sia ρ la relazione binaria in V definita ponendo, per ogni $x, y \in V$,

$$x\ \rho\ y \iff |x - y| = 2.$$

Disegnare il grafo $G = (V, \rho)$ (cioè il grafo su V che abbia ρ come relazione di adiacenza). G è connesso? È un albero? È una foresta?

Esercizio 6. Fornire, o spiegare perché non esistono, esempi di polinomi f tali che:

(1) $f \in \mathbb{R}[x]$, f ha grado 9, f non ha radici in $\mathbb{R}$;
(2) $f \in \mathbb{Q}[x]$, f ha grado 9, f non ha radici in $\mathbb{Q}$;
(3) $f \in \mathbb{R}[x]$, f ha grado 8, f non ha radici in $\mathbb{R}$;
(4) $f \in \mathbb{R}[x]$, f ha grado 8, f ha una ed una sola radice in $\mathbb{R}$;
(5) $f \in \mathbb{Q}[x]$, f ha grado 8, f è il prodotto di due polinomi irriducibili in $\mathbb{Q}[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
29 GENNAIO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Sia f l'applicazione $n \in \mathbb{N}^* \longmapsto \mathrm{rest}(8,n) \in \mathbb{N}$.

(*i*) Si determini l'immagine $\mathrm{im}\, f = \vec{f}(\mathbb{N}^*)$ di f.

(*ii*) Detto $\Re_f$ il nucleo di equivalenza di f, si studi l'insieme quoziente $\mathbb{N}^*/\Re_f$, descrivendone esplicitamente tutte le classi, ciascuna con i rispettivi elementi.

(*iii*) Sia Σ la relazione d'ordine definita in $\mathbb{N}^*$ ponendo, per ogni $n, m \in \mathbb{N}^*$,

$$n \,\Sigma\, m :\Longleftrightarrow\ n = m \text{ oppure } \mathrm{rest}(8,n) \text{ è un divisore proprio di } \mathrm{rest}(8,m).$$

Si determinino in $(\mathbb{N}^*, \Sigma)$ eventuali minimo, massimo, elementi minimali, elementi massimali.

(*iv*) Considerato il sottoinsieme $X = \{1,3,5,6,7,9\}$ di $\mathbb{N}^*$, si disegni il diagramma di Hasse di (X,Σ). Inoltre

(*a*) Per tutte le coppie $(x,y) \in X \times X$ di elementi non confrontabili tra loro, determinare $\inf\{x,y\}$ e $\sup\{x,y\}$.

(*b*) Spiegare perché (X,Σ) è un reticolo, e stabilire se è un reticolo complementato, determinando nel caso, per ogni $x \in X$, un complemento di x.

(*c*) Dedurre da (*b*) che (X,Σ) non è distributivo.

Esercizio 2. Si studi l'operazione binaria $*$ definita in $\mathbb{Z}_{210}$ ponendo, per ogni $a, b \in \mathbb{Z}_{210}$,

$$a * b = a + \overline{15}b.$$

(*i*) $*$ è commutativa? È associativa?

(*ii*) Esiste in $(\mathbb{Z}_{210}, *)$ un elemento neutro a destra, un elemento neutro a sinistra, un elemento neutro?

(*iii*) Si verifichi che $T := \{\overline{15z} \mid z \in \mathbb{Z}\}$ è una parte chiusa in $(\mathbb{Z}_{210}, *)$.

(*iv*) Che tipo di struttura è $(T, *)$? (un semigruppo, un monoide, un gruppo, nessuna di queste, ...; commutativa oppure no?).

(*v*) Determinare gli $n \in \mathbb{N}$ tali che $12 \leq n \leq 16$ e $\bar{n}$ sia invertibile in $(\mathbb{Z}_{210}, \cdot\,)$, calcolando $\bar{n}^{-1}$.

Esercizio 3.

(*i*) Si verifichi che il polinomio $f = x^2 + x + \bar{9} \in \mathbb{Z}_{11}[x]$ è l'associato monico di $g = \bar{4}x^2 + \bar{4}x + \bar{3}$, determinando $k \in \mathbb{Z}_{11}$ tale che $f = kg$.

(*ii*) Verificare che $I = \{sf \mid s \in \mathbb{Z}_{11}[x]\}$ coincide con $J = \{h \in \mathbb{Z}_{11}[x] \mid h(\bar{1}) = h(-\bar{2}) = \bar{0}\}$.

(*iii*) Determinate in I, se esiste,

(*a*) un polinomio h di grado 3 il cui insieme delle radici sia $\{\bar{1}, -\bar{2}\}$;

(*b*) un polinomio t di grado 3 che sia prodotto di due polinomi irriducibili;

(*c*) un polinomio irriducibile p di grado 3.

(*iv*) Dopo aver elencato in modo esplicito gli elementi del sottoinsieme $T = \{c^2 \mid c \in \mathbb{Z}_{11}\}$ di $\mathbb{Z}_{11}$ ed aver calcolato $|T|$, dire quali e quanti sono i polinomi *irriducibili* di $\mathbb{Z}_{11}[x]$ della forma $x^2 - a$, con $a \in \mathbb{Z}_{11}$.

(*v*) Nell'insieme J definito al punto (*ii*), si trovino, se possibile, polinomi u e v di grado 4 in modo che u sia il prodotto di due polinomi irriducibili e v sia il prodotto di tre polinomi irriducibili (in $\mathbb{Z}_{11}[x]$).

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO, GRUPPO RECUPERO)
15 FEBBRAIO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Scrivere la definizione di *partizione* di un insieme A. Se $|A| = 10$, il numero delle partizioni di A è maggiore, minore o uguale a 10?

Esercizio 2. (*i*) Elencare gli elementi di $S := \{a^2 \mid a \in \mathbb{Z}_{12}\}$ e determinare $|S|$.
(*ii*) Studiare iniettività e suriettività della funzione $f\colon (a,b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12} \mapsto a^2 + b^2 \in \mathbb{Z}_{12}$. *(Suggerimento: si tenga conto di $|S|$, calcolata al punto precedente.)*
(*iii*) Detto $\Re_f$ il nucleo di equivalenza di f, si calcoli $|\mathbb{Z}_{12} \times \mathbb{Z}_{12}/\Re_f|$ *(non c'è bisogno di elencare le classi o i loro elementi)*. Esiste in $[(\bar{1},\bar{0})]_{\Re_f}$ una coppia (a,b) tale che $a \neq \bar{0} \neq b$?

Esercizio 3. Si consideri in $\mathbb{N}^*$ la relazione binaria Σ definita ponendo, per ogni $a, b \in \mathbb{N}^*$,

$$a \,\Sigma\, b \iff a - 1 \mid b - 1.$$

(*i*) Verificare che Σ è una relazione d'ordine. Σ è totale?
(*ii*) Determinare in $(\mathbb{N}^*, \Sigma)$, se esistono, minimo, massimo, elementi minimali, elementi massimali.
(*iii*) Verificare che, per ogni $a, b \in \mathbb{N}^*$, posto $d = \mathrm{MCD}(a-1, b-1)$, in $(\mathbb{N}^*, \Sigma)$ si ha $\inf\{a, b\} = d+1$.
(*iv*) Posto $A = \{2, 3, 4, 5, 7, 13, 61\}$, si disegni il diagramma di Hasse di (A, Σ) e si determinino, in (A, Σ), eventuali minimo, massimo, elementi minimali, elementi massimali. (A, Σ) è un reticolo?
(*v*) Si trovi poi un $n \in \mathbb{N}^* \setminus A$ tale che $X := A \cup \{n\}$, ordinato da Σ, sia un reticolo complementato e non distributivo. Esiste un insieme Y tale che $(\mathcal{P}(Y), \subseteq)$ sia isomorfo a (X, Σ)?

Esercizio 4. Si consideri in $\mathbb{Z}_{27}$ il sottoinsieme $X = \{\bar{3}\bar{z} \mid z \in \mathbb{Z}\}$. Sia $*$ l'operazione binaria in X definita ponendo, per ogni $x, y \in X$, $x * y = xy + \bar{9}$.
(*i*) $*$ è associativa?
(*ii*) Esiste in $(X, *)$ un elemento neutro?
(*iii*) Determinare, se esiste, $t \in \mathbb{Z}$ tale che $\bar{6} * \bar{3}\bar{t} = \overline{15}$.
(*iv*) Determinare, se esiste, $t \in \mathbb{Z}$ tale che $\bar{6} * \bar{3}\bar{t} = \overline{18}$.

Esercizio 5.
(*i*) Si determinino $a, b \in \mathbb{Z}_5$ tali che il polinomio $f = \bar{3}ax^2 + \bar{2}ax + b \in \mathbb{Z}_5[x]$ sia monico e divisibile per $x - \bar{4}$.
(*ii*) Per i valori di a e b trovati al punto precedente, si scriva f come prodotto di fattori irriducibili in $\mathbb{Z}_5[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II , RECUPERO)
19 MARZO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Posto $S = \{2, 6, 10, 20\}$ e indicato con $\mathbb{P}$ l'insieme dei numeri naturali primi, si descrivano esplicitamente gli elementi di ciascuno degli insiemi:

$$A = \{p \in \mathbb{P} \mid (\exists x \in S)(p|x)\} \qquad B = \{p \in \mathbb{P} \mid (\exists x \in S)(p \nmid x)\}$$
$$C = \{p \in \mathbb{P} \mid (\forall x, y \in S)(p|x \Rightarrow p|y)\} \qquad D = \{\mathrm{MCD}(a, b) \mid (a, b) \in S \times S\}$$
$$E = \{\mathrm{rest}(a, 5) \mid a \in S\} \qquad F = \{\mathrm{rest}(a, b) \mid a, b \in S\}.$$

Esercizio 2. Per ogni $n \in \mathbb{N}^{\#}$ esiste una ed una sola coppia $(E(n), D(n)) \in \mathbb{N} \times \mathbb{N}^{\#}$ tale che $D(n)$ sia dispari e $n = 2^{E(n)}D(n)$. Dopo aver enunciato il Teorema Fondamentale dell'Aritmetica, giustificare questa affermazione.

Con le stesse notazioni, sia $*$ l'operazione binaria in $\mathbb{N}^{\#}$ definita ponendo, per ogni $a, b \in \mathbb{N}^{\#}$, $a * b = 2^{E(a)}D(b)$.

(*i*) $*$ è associativa?; $*$ è commutativa?; $*$ è iterativa (vale cioè $a * a = a$ per ogni $a \in \mathbb{N}^{\#}$)?
(*ii*) Esiste in $(\mathbb{N}^{\#}, *)$ un elemento neutro a destra, un elemento neutro a sinistra, un elemento neutro?
(*iii*) Tra le seguenti parti di $\mathbb{N}^{\#}$, dire quali sono chiuse e quali no: $2\mathbb{N}^{\#}$ (l'insieme degli interi positivi pari), $2\mathbb{N} + 1$ (l'insieme degli interi positivi dispari), $\{1, 2\}$, $\{2, 3\}$, $\{100\}$.
(*iv*) Esiste in $(2\mathbb{N} + 1, *)$ un elemento neutro a destra, un elemento neutro a sinistra, un elemento neutro?

Esercizio 3. Per ogni $n \in S := \mathbb{N}^{\#} \setminus \{1\}$, sia p_n il minimo primo positivo divisore di n. Si consideri l'applicazione $f\colon n \in S \mapsto n/p_n \in \mathbb{N}^{\#}$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Sia $\sim$ il nucleo di equivalenza di f. Si elenchino gli elementi di $[6]_\sim$ e di $[12]_\sim$; si descrivano in modo esplicito gli elementi di $[17]_\sim$.
(*iii*) È vero che $[4n]_\sim = \{4n\}$ per ogni $n \in \mathbb{N}^{\#}$?

Sia Σ la relazione d'ordine definita in S ponendo, per ogni $n, m \in S$, $n \,\Sigma\, m$ se e solo se o $n = m$ oppure $f(n)$ è un divisore proprio di $f(m)$.

(*iv*) Descrivere gli (eventuali) elementi minimali e massimali in (S, Σ), nonché gli eventuali minimo e massimo di (S, Σ).
(*v*) Determinare, in (S, Σ), l' insieme dei minoranti e quello dei maggioranti di $\{4, 6\}$.
(*vi*) (S, Σ) è un insieme totalmente ordinato? È un reticolo? Nel caso, è distributivo? È complementato?
(*vii*) Disegnare il diagramma di Hasse di $T = \{4, 6, 8, 13, 27, 72\} \subset S$, ordinato da Σ.
(*viii*) (T, Σ) è un insieme totalmente ordinato? È un reticolo? Nel caso, è distributivo? È complementato?

Esercizio 4. Per ogni primo (positivo) p, sia $f_p = \overline{20}x^4 - x^2 + \bar{3} \in \mathbb{Z}_p[x]$.

(*i*) Si determinino i primi p tali che f_p sia monico;
(*ii*) Si determinino i primi p tali che f_p abbia $-\bar{1}$ come radice;
(*iii*) Si determinino i primi p tali che f_p sia divisibile, in $\mathbb{Z}_p[x]$, per $g = x^2 - x - \bar{2}$, tenendo presente che $g = (x + \bar{1})(x - \bar{2})$.
(*iv*) Si determinino i primi p tali che f_p sia divisibile, in $\mathbb{Z}_p[x]$, per $h = x^3 - x^2 - \bar{2}x$, tenendo presente che $h = xg = x(x + \bar{1})(x - \bar{2})$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II , RECUPERO)
21 MAGGIO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Si dia la definizione di anello *booleano*. Tra $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}$ (con le consuete operazioni) e $(\mathcal{P}(\mathbb{Z}), \triangle, \cap)$ quali sono e quali non sono anelli booleani?

Esercizio 2. Per ogni $n \in \mathbb{N}$ si indichi con $\mathrm{uc}(n)$ l'ultima cifra nella scrittura decimale di n (ad esempio, $\mathrm{uc}(234) = 4$, $\mathrm{uc}(76) = 6$).

(*i*) Si trovi un $n \in \mathbb{N}$ tale che $\mathrm{uc}(n+1) \neq \mathrm{uc}(n) + 1$.

Si considerino le applicazioni

$$f\colon n \in \mathbb{N} \mapsto \mathrm{rest}(\mathrm{uc}(n), 7) \in \mathbb{N} \qquad \text{e} \qquad g\colon n \in \mathbb{N} \mapsto \mathrm{rest}(\mathrm{uc}(n), 13) \in \mathbb{N}.$$

(*ii*) Qual è il numero $|\operatorname{im} f|$ degli elementi dell'immagine di f?
(*iii*) Qual è il numero $|\operatorname{im} g|$ degli elementi dell'immagine di g?
(*iv*) Detti $\mathcal{R}_f$ e $\mathcal{R}_g$ rispettivamente i nuclei di equivalenza di f e g, indicare $|\mathbb{N}/\mathcal{R}_f|$ e $|\mathbb{N}/\mathcal{R}_g|$.
(*v*) Descrivere nel modo più esplicito possibile $[1]_{\mathcal{R}_f}$, $[4]_{\mathcal{R}_f}$ e, per ogni $n \in \mathbb{N}$, $[n]_{\mathcal{R}_g}$.

Sia ora ρ la relazione d'ordine definita in $S := \{n \in \mathbb{N} \mid n < 10\}$ ponendo, per ogni $a, b \in S$:

$$a \,\rho\, b \iff \big(a = b \vee (\, f(a) < f(b) \,\wedge\, g(a) < g(b)\,)\big).$$

(*vi*) Disegnare il diagramma di Hasse di (S, ρ).
(*vii*) (S, ρ) è un reticolo?
(*viii*) Descrivere in (S, ρ) l'insieme dei minoranti di $\{4, 8\}$ e quello dei maggioranti di $\{3, 7\}$.

Esercizio 3. Definiamo un grafo G sull'insieme di vertici $V = \{9, 10, 15, 20, 28, 10!\}$, dichiarando due elementi distinti a, b di V adiacenti se e solo se l'equazione congruenziale $ax \equiv_b 6$ ha soluzioni.

(*i*) Disegnare il grafo G.
(*ii*) G è connesso? G è un albero?
(*iii*) Quanti lati è necessario cancellare da G per ottenere una foresta (senza modificare l'insieme dei vertici)?

Esercizio 4. Sia K un campo. Per ogni polinomio non nullo $f \in K[x]$ indichiamo con $m(f)$ il polinomio monico associato ad f in $K[x]$, e poniamo anche $m(0) = 0$. Definamo l'operazione $*$ in $K[x]$ ponendo $f * g = m(fg)$ per ogni $f, g \in K[x]$.

(*i*) $*$ è associativa?, è commutativa?, ammette elemento neutro?

Per arbitrari $f, g \in K[x]$:

(*ii*) qualunque sia K, cosa possiamo dire sul massimo comun divisore, nell'anello $K[x]$, tra f e $f * g$?
(*iii*) se $K = \mathbb{Q}$, è vero che $(f + f) * g = f * g$?
(*iv*) se $K = \mathbb{Q}$, $(K[x], +, *)$ è un anello?

Nel caso in cui $K = \mathbb{Z}_7$, trovare, se esiste, un polinomio monico $f \in K[x]$ tale che

$$f * (\bar{3}x + \bar{2}) = x^3 + x + \bar{2}.$$

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II , RECUPERO)
20 GIUGNO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Si consideri l'applicazione $f\colon (a,b) \in \mathbb{N}\times\mathbb{N} \longmapsto a^2+b^2 \in \mathbb{N}$. Sia $\mathcal{R}_f$ il nucleo di equivalenza di f.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Si determinino gli elementi di: $[(0,0)]_{\mathcal{R}_f}$, $[(2,0)]_{\mathcal{R}_f}$, $[(3,4)]_{\mathcal{R}_f}$.
(*iii*) Caratterizzare le coppie $(a,b) \in \mathbb{N}\times\mathbb{N}$ tali che a^2+b^2 sia pari.

Si consideri ora la relazione d'ordine Σ_f definita ponendo, per ogni $a,b,c,d \in \mathbb{N}$,

$$(a,b)\ \Sigma_f\ (c,d) \iff (a,b)=(c,d) \vee f(a,b) < f(c,d).$$

(*iv*) Σ_f è di ordine totale?
(*v*) Si determinino in $(\mathbb{N}\times\mathbb{N},\Sigma_f)$ gli eventuali minimo, massimo, elementi minimali, elementi massimali.
(*vi*) Disegnare il diagramma di Hasse di (X,Σ_f), dove

$$X=\{(7,2),(6,0),(6,1),(1,1),(1,0),(3,4),(4,3),(5,0)\}.$$

(*vii*) (X,Σ_f) è un reticolo? Se lo è, è distributivo?, è complementato?

Esercizio 2. In $S=\mathbb{Z}_7\times\mathbb{Z}_{10}$ si consideri l'operazione $*$ così definita: per ogni $(\bar{a},\hat{b}),(\bar{c},\hat{d}) \in S$,

$$(\bar{a},\hat{b})*(\bar{c},\hat{d})=(\bar{a}+\bar{c}+\bar{2},\hat{9}\hat{b}\hat{d}).$$

(*i*) Si verifichi che $(S,*)$ è un monoide commutativo;
(*ii*) se ne determinino gli elementi invertibili. Si determini, in particolare, il simmetrico di $(\bar{7},\hat{7})$, mediante un'opportuna equazione congruenziale.
(*iii*) Stabilire se la parte $\mathbb{Z}_7\times\{\hat{1},\hat{9}\}$ è chiusa rispetto a $*$.

Esercizio 3. Dire quali delle seguenti affermazioni sono vere per ogni insieme ordinato $(X,\leq)$, giustificando le risposte:

(a) Se X è un reticolo, in X esistono $\sup X$ e $\inf X$.
(b) Se X ha massimo e minimo, X è un reticolo.
(c) Se X è un reticolo e $|X|=8$, X è un reticolo booleano.
(d) Se X è un reticolo finito e $|X|$ non è potenza di 2, X non è booleano.
(e) Se X è un reticolo complementato, ogni suo elemento ha un unico complemento.
(f) Se X è un reticolo booleano, ogni suo elemento ha un unico complemento.

Esercizio 4. Per ogni numero primo (positivo) p sia f_p il polinomio $\overline{30}x^4+\overline{16}x^3+\overline{2}x^2-x+\overline{1} \in \mathbb{Z}_p[x]$. Si trovi il primo p per il quale f_p sia monico di grado 3 ed abbia $\overline{1}$ come radice. Per tale valore di p, scrivere f_p come prodotto di polinomi monici irriducibili in $Z_p[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 LUGLIO 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Fornire la definizione di *partizione* di un insieme.
Sia $S = \{n \in \mathbb{N} \mid n < 10\}$ e siano $A = \{1, 2, 5, 8\}$, $B = \{0, 3, 9\}$ e $C = \{4, 6, 7\}$.
(*i*) $F := \{A, B, C\}$ è una partizione di S?
(*ii*) Esiste una relazione di equivalenza σ di S tale che $F = S/\sigma$?
(*iii*) Se tale σ esiste, si ha $1\ \sigma\ 2$? Si ha $3\ \sigma\ 4$? Elencare gli elementi di $[0]_\sigma$.
(*iv*) Quanti (e, nel caso esistano, quali) sono gli insiemi X tali che $\{A, X\}$ sia una partizione di S?

Esercizio 2. In $\mathbb{Z}_{10}$ si definisca l'operazione $*$ ponendo, per ogni $a, b \in \mathbb{Z}_{10}$, $\quad a * b = \bar{5}a + \bar{6}ab$.
(*i*) $*$ è commutativa? $*$ è associativa?
(*ii*) Si trovino i due elementi neutri a destra in $(\mathbb{Z}_{10}, *)$ [*Suggerimento:* $\bar{6}$ *è un divisore dello zero in* $(\mathbb{Z}_{10}, +, \cdot)$]. $(\mathbb{Z}_{10}, *)$ ha elementi neutri?
(*iii*) Siano $P = \{[n]_{10} \mid n \text{ è un intero pari}\}$ e $D = \{[n]_{10} \mid n \text{ è un intero dispari}\}$. P è una parte chiusa in $(\mathbb{Z}_{10}, *)$? D è una parte chiusa in $(\mathbb{Z}_{10}, *)$?

Esercizio 3. Verificare che la relazione binaria $\mathcal{R}$ definita in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$,

$$a\ \mathcal{R}\ b \iff (a = b \vee a^2 \mid b)$$

è una relazione d'ordine.
(*i*) $\mathcal{R}$ è di ordine totale?
(*ii*) Determinare in $(\mathbb{N}, \mathcal{R})$ gli eventuali minimo, massimo, elementi minimali, elementi massimali.
(*iii*) Disegnare il diagramma di Hasse di $(X, \mathcal{R})$, dove $X = \{0, 1, 2, 7, 8, 20, 250, 6400\}$.
(*iv*) $(X, \mathcal{R})$ è un reticolo? Se lo è, è distributivo? È complementato?

Esercizio 4. Determinare l'insieme di tutte le soluzioni (in $\mathbb{Z}$) dell'equazione congruenziale

$$30x \equiv_{38} 6.$$

Esercizio 5. Si trovi, se possibile, un polinomio monico $f \in \mathbb{Z}_5[x]$ di terzo grado che abbia $\bar{0}$, $\bar{1}$ e $-\bar{1}$ come radici. Tale f è unico?
(*i*) $f + (x + \bar{1})$ è multiplo di $x + \bar{1}$ in $\mathbb{Z}_5[x]$?
(*ii*) $f + (x + \bar{1})$ è irriducibile in $\mathbb{Z}_5[x]$?
(*iii*) $f + (x + \bar{2})$ è irriducibile in $\mathbb{Z}_5[x]$? (Suggerimento: basta stabilire se $\bar{2}$ è o non è radice di questo polinomio; come mai?)
(*iv*) Determinare l'insieme degli $a \in \mathbb{Z}_5$ tali che $f + a$ sia irriducibile in $\mathbb{Z}_5[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
5 SETTEMBRE 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Fornire la definizione di applicazione *iniettiva* e di applicazione *suriettiva*. Di ciascuna delle due applicazioni

$$f\colon A \in \mathcal{P}(\mathbb{Z}) \mapsto \mathbb{N} \smallsetminus A \in \mathcal{P}(\mathbb{Z}) \qquad \text{e} \qquad g\colon A \in \mathcal{P}(\mathbb{N}) \mapsto \mathbb{N} \smallsetminus A \in \mathcal{P}(\mathbb{Z}).$$

dire se è iniettiva e se è suriettiva.

Esercizio 2. In $\mathbb{Z}_{10}$ si definisca l'operazione $*$ ponendo, per ogni $a, b \in \mathbb{Z}_{10}$, $\quad a*b = \bar{3}ab + \bar{2}a - \bar{3}b + \bar{4}$.

(*i*) $*$ è commutativa? $*$ è associativa?
(*ii*) Siano $P = \{[n]_{10} \mid n \text{ è un intero pari}\}$ e $D = \{[n]_{10} \mid n \text{ è un intero dispari}\}$. P è una parte chiusa in $(\mathbb{Z}_{10}, *)$? D è una parte chiusa in $(\mathbb{Z}_{10}, *)$?
(*iii*) Si trovino, se esistono, tutti e soli gli $a \in \mathbb{Z}_{10}$ tali che $a * \bar{0} = \bar{0}$ ed i $b \in \mathbb{Z}_{10}$ tali che $\bar{0} * b = \bar{0}$.
(*iv*) Usando il risultato di (*iii*), stabilire se esiste in $(\mathbb{Z}_{10}, *)$ elemento neutro.

Esercizio 3.

(*i*) Dato un monoide $(M, \cdot)$, è sempre vero che l'insieme U degli elementi invertibili di M ne costituisce una parte chiusa? E, nel caso lo sia, U, munito dell'operazione indotta, è necessariamente un gruppo?
(*ii*) Si elenchino gli elementi di $\mathcal{U}(\mathbb{Z}_9)$, l'insieme degli invertibili di $(\mathbb{Z}_9, \cdot)$.

Si definisca in $\mathbb{Z}_9$ la relazione binaria ρ ponendo, per ogni $a, b \in \mathbb{Z}_9$,

$$a \,\rho\, b \iff (\exists u \in \mathcal{U}(\mathbb{Z}_9))(ua = b).$$

(*iii*) Stabilire se ρ è una relazione di equivalenza.
(*iv*) Nel caso in cui ρ sia di equivalenza, elencare gli elementi di $[\bar{0}]_\rho$, $[\bar{1}]_\rho$, $[\bar{2}]_\rho$, $[\bar{3}]_\rho$; elencare poi gli elementi di $\mathbb{Z}_9/\rho$ e dire quanto vale $|\mathbb{Z}_9/\rho|$.

Esercizio 4. Si verifichi che la relazione $\mathcal{R}$, definita in $\mathcal{P}(\mathbb{N})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{N})$,

$$X \,\mathcal{R}\, Y \iff X \subseteq Y \wedge |Y \smallsetminus X| \neq 1,$$

è una relazione d'ordine.

(*i*) $\mathcal{R}$ è di ordine totale?
(*ii*) Determinare in $(\mathcal{P}(\mathbb{N}), \mathcal{R})$ gli eventuali minimo, massimo, elementi minimali, elementi massimali.
(*iii*) Posto $X = \{0, 1, 2\}$, disegnare il diagramma di Hasse di $(\mathcal{P}(X), \mathcal{R})$.
(*iv*) $(\mathcal{P}(X), \mathcal{R})$ è un reticolo? Se lo è, è distributivo? È complementato?
(*v*) Indicare, se possibile, una parte P di $\mathcal{P}(\mathbb{N})$ tale che $|P| = 4$ e $(P, \mathcal{R})$ sia un reticolo booleano.

Esercizio 5. Si determini un primo p tale che il polinomio $f = \overline{10}x^4 + \bar{6}x^3 + \bar{3}x - \bar{6} \in \mathbb{Z}_p[x]$ sia monico di terzo grado.

(*i*) Tale p è univocamente determinato?
(*ii*) Decomporre f in prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$?
(*iii*) Esiste in $\mathbb{Z}_p[x]$ un polinomio irriducibile di secondo grado che divida f?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
17 OTTOBRE 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Sia $F = \mathcal{P}_{\mathrm{f}}(\mathbb{N})$ l'insieme delle parti finite di $\mathbb{N}$, e sia f l'applicazione

$$f\colon X \in F \longmapsto \begin{cases} \varnothing, & \text{se } X = \varnothing \\ X \smallsetminus \{\min X, \max X\}, & \text{se } X \neq \varnothing \end{cases} \in F.$$

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Caratterizzare gli $X \in F$ tali che ...
  (a) ... $f(X) = \varnothing$;
  (b) ... $|X| = |f(X)|$;
  (c) ... $|X| = |f(X)| + 1$.

Sia $\mathcal{R}$ la relazione d'ordine in F definita da: $\forall X, Y \in F$

$$X \mathcal{R} Y \iff (X = Y \vee f(X) \subset f(Y)).$$

(*iii*) $\mathcal{R}$ è totale?
(*iv*) Caratterizzare gli eventuali elementi minimali, massimali, minimo, massimo in $(F, \mathcal{R})$.

Posto $S = \{1, 2, 3, 4\}$, studiare la relazione d'ordine indotta da $\mathcal{R}$ su $\mathcal{P}(S)$:

(*v*) elencare gli eventuali elementi minimali, massimali, minimo, massimo in $(\mathcal{P}(S), \mathcal{R})$;
(*vi*) $(\mathcal{P}(S), \mathcal{R})$ è un reticolo?

Posto $T = \{\varnothing, S\} \cup \{S \smallsetminus \{x\} \mid x \in S\}$, studiare la relazione d'ordine indotta da $\mathcal{R}$ su T:

(*vii*) disegnare il diagramma di Hasse di $(T, \mathcal{R})$;
(*viii*) $(T, \mathcal{R})$ è un reticolo?

Esercizio 2. In $\mathbb{Q}^* \times \mathbb{Q}$ si definisca l'operazione $*$ ponendo, per ogni $(a, b), (c, d) \in \mathbb{Q}^* \times \mathbb{Q}$,

$$(a, b) * (c, d) = (ac, ad + b).$$

(*i*) $*$ è commutativa? $*$ è associativa?
(*ii*) $(\mathbb{Q}^* \times \mathbb{Q}, *)$ ha elemento neutro? Nel caso lo abbia, dire quali elementi di $\mathbb{Q}^* \times \mathbb{Q}$ sono invertibili rispetto a $*$, descrivendone esplicitamente gli inversi.
(*iii*) $(\mathbb{Q}^* \times \mathbb{Q}, *)$ è un semigruppo?, un monoide?, un gruppo?
(*iv*) Per ciascuno di $\mathbb{Z}^* \times \mathbb{Q}$, $\mathbb{Q}^* \times \mathbb{Z}$ e $\{1, -1\} \times \mathbb{Z}$ si stabilisca se è o meno una parte chiusa in $(\mathbb{Q}^* \times \mathbb{Q}, *)$ e, nel caso lo sia, dedurre dai risultati precedenti che genere di struttura costituisca con l'operazione indotta da $*$.

Esercizio 3. Si determini l'insieme degli interi n tali che $10 \leq n \leq 18$ e l'equazione congruenziale $2nx \equiv_{108} 6$ abbia soluzioni. Si determini l'insieme di tutte le soluzioni nel caso in cui n sia il minimo tale intero.

Esercizio 4. Per definizione, se $f \in \mathbb{Q}[x]$, cosa significa dire che un polinomio $g \in \mathbb{Q}[x]$ è *associato* a f in $\mathbb{Q}[x]$? È vero che ogni polinomio non nullo in $\mathbb{Q}[x]$ ha (in $\mathbb{Q}[x]$) un associato di coefficiente direttore $5/2$?

Esiste o non esiste (se esiste, fornire un esempio):

(*i*) $f \in \mathbb{Q}[x]$ tale che $f(1) = f(2) = f(3) = 0$, f abbia grado 4 ed f abbia in $\mathbb{Q}[x]$ un divisore irriducibile di secondo grado?
(*ii*) $f \in \mathbb{Q}[x]$, di grado 9, i cui fattori irriducibili in $\mathbb{Q}[x]$ abbiano tutti grado pari?
(*iii*) $f \in \mathbb{Q}[x]$, di grado 5, privo di radici in $\mathbb{Q}$, che abbia in $\mathbb{Q}[x]$ un divisore irriducibile di grado 4?
(*iv*) $f \in \mathbb{Q}[x]$, di grado 5, che abbia 0 come unica radice in $\mathbb{Q}$ e che abbia in $\mathbb{Q}[x]$ un divisore irriducibile di grado 3?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
14 NOVEMBRE 2013

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare le definizioni di: *anello*, *campo*, *dominio di integrità*. Fornire, se esistono (ma, in caso contrario, spiegare perché non esistono) esempi di:

(*i*) un anello che non sia un campo;
(*ii*) un campo che non sia un dominio di integrità;
(*iii*) un dominio di integrità che non sia un campo;
(*iv*) un anello infinito che non sia un dominio di integrità.

Esercizio 2. Rappresentare su un diagramma di Venn di tipo generale l'espressione insiemistica $(A \smallsetminus B) \triangle (B \cup C)$.

Esercizio 3. È dato il semigruppo $(S, *)$, dove $S = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ e, per ogni $(a_1, b_1, c_1), (a_2, b_2, c_2) \in S$,

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, a_1b_2 + b_1c_2, c_1c_2).$$

(*i*) $*$ è commutativa?
(*ii*) $(S, *)$ ha elemento neutro? Nel caso lo abbia, dire quali elementi di S sono invertibili rispetto a $*$, descrivendone esplicitamente gli inversi.
(*iii*) $(S, *)$ è un monoide? $(S, *)$ è un gruppo?
(*iv*) $T := \{(a, b, 0) \mid a, b \in \mathbb{R}\}$ è una parte chiusa in $(S, *)$? Nel caso lo sia, $(T, *)$ è un semigruppo commutativo? È un monoide? È un gruppo?

Esercizio 4. Per ogni $n \in \mathbb{N}$, si indichi con $c(n)$ l'insieme delle cifre nella rappresentazione decimale di n (dunque, ad esempio, $c(2303) = \{0, 2, 3\}$, $c(8) = \{8\}$). Definita l'applicazione

$$f \colon n \in \mathbb{N} \mapsto (\min c(n), \max c(n)) \in \mathbb{N} \times \mathbb{N},$$

sia ρ il nucleo di equivalenza di f.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Esistono numeri naturali n tali che $|[n]_\rho| = 1$? Caratterizzare tali n.
(*iii*) Descrivere in modo esplicito $[10]_\rho$.

Sia σ la relazione d'ordine definita in $\mathbb{N}$ da: $\forall n, m \in \mathbb{N}$

$$n \; \sigma \; m \iff \big(n = m \vee \max c(n) < \max c(m)\big).$$

(*iv*) Caratterizzare gli eventuali elementi minimali, massimali, minimo, massimo in $(\mathbb{N}, \sigma)$.
(*v*) $(\mathbb{N}, \sigma)$ è un reticolo?
(*vi*) Determinare in $(\mathbb{N}, \sigma)$ una parte totalmente ordinata massimale.
(*vii*) Disegnare il diagramma di Hasse di $A := \{11010001, 123, 31, 40\}$, ordinato da σ.
(*viii*) (A, σ) è un reticolo? Nel caso lo sia, è distributivo?, è complementato?, è booleano?

Esercizio 5. Per ogni naturale primo p sia $f_p = \bar{7}x^4 + \bar{5}x^3 - \bar{2} \in \mathbb{Z}_p[x]$.

(*i*) Risolvendo un'opportuna equazione congruenziale, si determini, se esiste, un associato monico di f_{17} in $\mathbb{Z}_{17}[x]$.
(*ii*) Si scriva f_5 come prodotto di un invertibile e di polinomi monici irriducibii in $\mathbb{Z}_5[x]$.
(*iii*) Si scriva f_3 come prodotto di un invertibile e di polinomi monici irriducibii in $\mathbb{Z}_3[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 DICEMBRE 2013

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte.* Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Per definizione, quando è che un elemento a di un semigruppo $(S, *)$ si dice cancellabile? È vero che, in un monoide, ogni elemento simmetrizzabile è cancellabile? È vero che, in un monoide, ogni elemento cancellabile è simmetrizzabile?

Nel monoide $(\mathcal{P}(\mathbb{Z}), \cup)$), l'elemento $\mathbb{N}$ è cancellabile?

Esercizio 2. È data l'applicazione $f\colon n \in \mathbb{Z} \mapsto \bar{6}\bar{n}^2 + \bar{4} \in \mathbb{Z}_{10}$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Descrivere in modo esplicito $[0]_\rho$ e $[1]_\rho$, dove ρ è il nucleo di equivalenza di f.

Esercizio 3. Per ogni $X \in \mathcal{P}(\mathbb{N})$ si definisca in $\mathbb{N}$ la relazione binaria $\mathcal{R}_X$ ponendo, per ogni $a, b \in \mathbb{N}$:

$$a \,\mathcal{R}_X\, b \iff (\exists x \in X)(b = ax).$$

(*i*) È vero che, per ogni scelta di X, la relazione $\mathcal{R}_X$ è antisimmetrica?
(*ii*) Caratterizzare le parti X di $\mathbb{N}$ tali che $\mathcal{R}_X$ sia riflessiva.
(*iii*) Caratterizzare le parti X di $\mathbb{N}$ tali che $\mathcal{R}_X$ sia transitiva. [Suggerimento: siano $a, b \in X$; allora $1\ \mathcal{R}_X\ a$ e $a\ \mathcal{R}_X\ ab$. Se $\mathcal{R}_X$ è transitiva, quale conseguenza se ne trae?]

Avendo posto $A = 2\mathbb{N}$ (l'insieme dei naturali pari), $B = \mathbb{N} \smallsetminus 2\mathbb{N}$ (l'insieme dei naturali dispari) e $C = \{n \in \mathbb{N} \mid n > 10\}$, esattamente uno tra A, B e C, chiamiamolo T, ha la proprietà che $\mathcal{R}_T$ sia una relazione d'ordine.

(*iv*) Quale tra A, B e C è T?
(*v*) Caratterizzare in $(\mathbb{N}, \mathcal{R}_T)$ gli eventuali elementi minimali, massimali, minimo, massimo;
(*vi*) indicare se esistono (o spiegare perché non esistono) $\inf\{18, 30\}$ e $\sup\{18, 20\}$ in $(\mathbb{N}, \mathcal{R}_T)$;
(*vii*) $(\mathbb{N}, \mathcal{R}_T)$ è un reticolo? Nel caso lo sia, è distributivo? È complementato? È booleano?
(*viii*) Se $S = \{0, 1, 2, 6, 9, 18\}$ e $X = \mathbb{N} \smallsetminus \{2, 4, 5, 121\}$, $\mathcal{R}_X$ induce una relazione d'ordine su S. Disegnare il diagramma di Hasse di $(S, \mathcal{R}_X)$;
(*ix*) $(S, \mathcal{R}_X)$ è un reticolo?
(*x*) Esiste un elemento $x \in S$ tale che $S \smallsetminus \{x\}$, ordinato dalla relazione indotta da $\mathcal{R}_X$, sia un reticolo? (Nel caso, indicare un tale x?). Questo reticolo è distributivo?
(*xi*) Esistono $x, y \in S$ tali che $S \smallsetminus \{x, y\}$, ordinato dalla relazione indotta da $\mathcal{R}_X$, sia un reticolo booleano? (Nel caso, indicare tali x e y).

Esercizio 4. Per ogni $f \in \mathbb{Q}[x]$, sia $R(f) = \{c \in \mathbb{Q} \mid f(c) = 0\}$, l'insieme delle radici razionali di f.

(*i*) È vero che, per ogni $f, g \in \mathbb{Q}[x]$, se f divide g (in $\mathbb{Q}[x]$) allora $R(f) \subseteq R(g)$?
(*ii*) Viceversa, è vero che, per ogni $f, g \in \mathbb{Q}[x]$, se $R(f) \subseteq R(g)$ allora f divide g (in $\mathbb{Q}[x]$)?
(*iii*) Trovare, se esiste, un polinomio $h \in \mathbb{Q}[x]$ di grado 5 tale che $|R(h)| = 1$ e h non abbia divisori irriducibili di grado maggiore di 1.
(*iv*) Descrivere esplicitamente l'insieme $A = \big\{g \in \mathbb{Q}[x] \mid \{1, -1\} \subseteq R(g)\big\}$.

Si definisca un'operazione binaria $*$ in $\mathbb{Q}[x]$ ponendo, per ogni f, $g \in \mathbb{Q}[x]$,

$$f * g = \begin{cases} \prod_{c \in R(g)} (x - c) & \text{se } R(g) \neq \varnothing \\ 1 & \text{se } R(g) = \varnothing. \end{cases}$$

(*v*) $*$ è commutativa? $*$ è associativa?
(*vi*) $(\mathbb{Q}[x], *)$ ha elementi neutri a destra? Ha elementi neutri a sinistra? Ha elemento neutro?
(*vii*) L'insieme dei polinomi monici in $\mathbb{Q}[x]$ è una parte chiusa rispetto a $*$?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
28 GENNAIO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Per definizione, cosa è un *albero*? Sia T è un albero con esattamente 125 vertici e n lati. Cosa sappiamo dire su n?

Esercizio 2. Per ogni parte non vuota X di $\mathbb{N}$, sia $\pi(X) = \{p \in \mathbb{P} \mid (\exists x \in X)(p|x)\}$ (come di consueto, indichiamo con $\mathbb{P}$ l'insieme dei numeri naturali primi). Posto $M = \{x \in \mathbb{N} \mid x \geq 2\}$ si consideri l'applicazione

$$f\colon X \in \mathcal{P}(M) \smallsetminus \{\varnothing\} \longmapsto \min \pi(X) \in \mathbb{P}.$$

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Calcolare $f(D)$, dove D è l'insieme dei numeri interi dispari maggiori di 1, e $f(3\mathbb{N}^{\#})$.
(*iii*) Descrivere in modo esplicito $[\{6\}]_{\sim}$, dove $\sim$ è il nucleo di equivalenza di f.

Si definisca in $S := \mathcal{P}(M) \smallsetminus \{\varnothing\}$ la relazione d'ordine $\mathcal{R}$ ponendo, per ogni $X, Y \in \mathcal{R}$:

$$X \mathcal{R} Y \iff (X = Y \vee f(X) < f(Y)).$$

(*iv*) Determinare in $(S, \mathcal{R})$ gli eventuali elementi minimali, massimali, minimo, massimo.
(*v*) Sia $A = \{\{7, 9\}, \{11, 15\}\}$. In $(S, \mathcal{R})$, descrivere l'insieme dei minoranti di A, l'insieme dei maggioranti di A e, se esistono, $\inf A$ e $\sup A$.
(*vi*) $(S, \mathcal{R})$ è un reticolo?
(*vii*) Sia $B = \{\{2, 5\}, \{7, 9\}, \{11, 15\}, \{7, 11\}, \{11, 13, 29\}\}$. Disegnare il diagramma di Hasse di $(B, \mathcal{R})$. $(B, \mathcal{R})$ è un reticolo? Nel caso lo sia, è distributivo? È complementato? È booleano?
(*viii*) Esiste un insieme finito C tale che $(B, \mathcal{R})$ sia isomorfo a $(\mathcal{P}(C), \subseteq)$?

Esercizio 3. Si consideri il semigruppo commutativo $(\mathbb{R} \times \mathbb{R}, *)$, dove, per ogni $a, b, c, d \in \mathbb{R}$,

$$(a, b) * (c, d) = (ac + 2bd, ad + bc).$$

(*i*) Verificare che $(\mathbb{R} \times \mathbb{R}, *)$ è un monoide.
(*ii*) Determinare, se esistono, gli inversi in $(\mathbb{R} \times \mathbb{R}, *)$ di $(2, 2)$ e $(\sqrt{2}, 1)$.
(*iii*) $\mathbb{R} \times \{0\}$ è una parte chiusa rispetto a $*$? Se sì, $(\mathbb{R} \times \{0\}, *)$ è isomorfo a $(\mathbb{R}, \cdot)$?
(*iv*) $\{0\} \times \mathbb{R}$ è una parte chiusa rispetto a $*$? Se sì, $(\{0\} \times \mathbb{R}, *)$ è isomorfo a $(\mathbb{R}, \cdot)$?

Esercizio 4. Stabilire per quali interi $m > 1$ esiste $\bar{a} \in \mathbb{Z}_m$ tale che

$$\bar{4}\bar{a} + \bar{3} = \bar{5} + \bar{7}. \qquad (\diamond)$$

Detto n il minimo tale intero m che sia compreso tra 10 e 20, si determini $\bar{a} \in \mathbb{Z}_n$ che soddisfi $(\diamond)$.

Esercizio 5.

(*i*) È vero che ogni polinomio di grado 11 in $\mathbb{Q}[x]$ ha almeno una radice in $\mathbb{R}$?
(*ii*) È vero che ogni polinomio di grado 11 in $\mathbb{Q}[x]$ ha almeno una radice in $\mathbb{Q}$?
(*iii*) Trovare, se esiste (o, in caso contrario, spiegare perché non esiste), un polinomio $f \in \mathbb{R}[x]$ di grado 8 che sia il prodotto di due polinomi irriducibili.
(*iv*) Trovare, se esiste (o, in caso contrario, spiegare perché non esiste), un polinomio $g \in \mathbb{Q}[x]$ di grado 8 che sia il prodotto di due polinomi irriducibili.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
18 FEBBRAIO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte.* Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Fornire la definizione di *partizione* di un insieme S.
Sia A un insieme. Se $|A| = 4$, quante sono le partizioni F di A tali che $|F| = 2$?

Esercizio 2. Siano α e β le relazioni binarie definite in $\mathbb{Z}$ ponendo, per ogni $n, m \in \mathbb{Z}$

$$n \,\alpha\, m \iff \big(n = m \ \vee\ (\mathrm{rest}(n,7) + \mathrm{rest}(m,7) = 7)\big);$$
$$n \,\beta\, m \iff \big(n \equiv_7 m \vee\ (\mathrm{rest}(n,7) + \mathrm{rest}(m,7) = 7)\big).$$

Dimostrare che esattamente una tra α e β è una relazione di equivalenza. Quale? Con riferimento a questa equivalenza, descrivere in modo esplicito l'insieme quoziente e le classi di equivalenza. Quanti sono gli elementi dell'insieme quoziente?

Esercizio 3. Per ogni $n \in \mathbb{Z}$, sia $\pi(n) = \{p \in \mathbb{P} \mid p|n\}$, dove $\mathbb{P}$ è l'insieme dei numeri interi primi positivi. Sia σ la relazione d'ordine in $\mathbb{Z}$ definita da:

$$(\forall a, b \in \mathbb{Z})(a \,\sigma\, b \iff (a \leq b \wedge \pi(a) \subseteq \pi(b))).$$

(*i*) σ è totale?
(*ii*) Determinare in $(\mathbb{Z}, \sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
(*iii*) $(\mathbb{Z}, \sigma)$ è un reticolo?
(*iv*) Sia $A = \{10, 12\}$. Descrivere, in $(\mathbb{Z}, \sigma)$, l'insieme dei minoranti di A, e, se esiste, $\inf A$.

Sia $S = \{-1, 0, 1, 2, 3, 4, 10, 12, 30, 60\}$.

(*v*) Disegnare il diagramma di Hasse di (S, σ).
(*vi*) (S, σ) è un reticolo? Nel caso lo sia, è distributivo? È complementato? È booleano?
(*vii*) Dimostrare che esiste un unico $x \in S$ tale che $(S \smallsetminus \{x\}, \sigma)$ sia un reticolo. Questo reticolo è distributivo? È complementato? È booleano?
(*viii*) Esistono $x, y \in S$ tali che $(S \smallsetminus \{x, y\}, \sigma)$ sia un reticolo booleano? Nel caso, trovare tali x e y.

Esercizio 4.

(*i*) Trovare l'insieme delle soluzioni (in $\mathbb{Z}$) dell'equazione congruenziale $8x \equiv_{34} 2$.
(*ii*) Per ogni $k \in \mathbb{Z}_{17}$, si consideri l'applicazione $f_k \colon \bar{n} \in \mathbb{Z}_{17} \mapsto \bar{n}(\bar{4}k - \bar{1}) \in \mathbb{Z}_{17}$. Tenendo presente quanto al punto precedente, dire per quali, e quanti, valori di k l'applicazione f_k è iniettiva e per quali, e quanti, valori di k l'applicazione f_k è suriettiva.

Esercizio 5. Per ogni primo p sia f_p il polinomio $x^4 + 5x^3 - 10x^2 - 4x + 1 \in \mathbb{Z}_p[x]$. Fattorizzare in prodotto di polinomi irriducibili:

(*i*) f_5 in $\mathbb{Z}_5[x]$;
(*ii*) f_3 in $\mathbb{Z}_3[x]$;
(*iii*) f_2 in $\mathbb{Z}_2[x]$. Tenere presente il fatto che $x^2 + x + 1$ è l'unico polinomio irriducibile di grado 2 in $\mathbb{Z}_2[x]$.

Si ricorda che è parte essenziale dell'esercizio la giustificazione del fatto che i fattori indicati come tali siano effettivamente irriducibili.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
18 MARZO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Fornire le definizioni di *dominio di integrità* e di *campo*. Se possibile, fornire esempi di:

(*i*) un dominio di integrità che non sia un campo;
(*ii*) un campo che non sia un dominio di integrità;
(*iii*) un anello che non sia un dominio di integrità.

Esercizio 2. Posto $S = \{n \in \mathbb{N} \mid n \leq 10\}$, per ogni parte X di S si ponga $\hat{X} = \{10 - x \mid x \in X\}$ e si consideri l'applicazione $f\colon X \in \mathcal{P}(S) \mapsto \hat{X} \in \mathcal{P}(S)$.

(*i*) Determinare $f(\{1\})$, $f(\{5,7\})$ e $f(S)$;
(*ii*) f è iniettiva?
(*iii*) f è suriettiva?
(*iv*) Calcolare l'applicazione composta $f \circ f$.

Detto $\mathcal{R}$ il nucleo di equivalenza di f, si descrivano gli elementi di $\mathcal{P}(S)/\mathcal{R}$ e si calcoli $|\mathcal{P}(S)/\mathcal{R}|$.

Esercizio 3. Vero o falso? Tutte le frasi sono riferite ad un insieme ordinato (non vuoto) $(X, \leq)$.

(*i*) Se $(X, \leq)$ è un reticolo, certamente esistono $\inf X$ e $\sup X$.
(*ii*) Se esistono $\inf X$ e $\sup X$, allora certamente $(X, \leq)$ è un reticolo.
(*iii*) Se $(X, \leq)$ è un reticolo finito, certamente esistono $\inf X$ e $\sup X$.
(*iv*) Se $(X, \leq)$ è limitato e totalmente ordinato, e se $|X| > 2$, allora X non può essere complementato.
(*v*) Se $(X, \leq)$ è totalmente ordinato, allora sicuramente X è distributivo.
(*vi*) Se $(X, \leq)$ è un reticolo finito e $|X|$ è una potenza di 2, allora X è necessariamente booleano.
(*vii*) Se $(X, \leq)$ è un reticolo finito booleano, allora $|X|$ è necessariamente una potenza di 2.

Esercizio 4. Si definiscano, nel prodotto cartesiano $R := \mathbb{Z}_6 \times \mathbb{Z}_{19}$ due operazioni binarie $\oplus$ e $*$ ponendo, per ogni $a, c \in \mathbb{Z}_6$ e $b, d \in \mathbb{Z}_{19}$, $(a,b) \oplus (c,d) = (a+c, b+d)$ e $(a,b) * (c,d) = (ac, bd)$. Verificare che $(R, \oplus, *)$ è un anello commutativo unitario.

(*i*) Determinare gli invertibili ed in divisori dello zero in $(R, \oplus, *)$, indicandone anche il numero. Verificare che tutti gli elementi non nulli e non invertibili sono divisori dello zero.
(*ii*) Determinare tutti e soli gli $(x, y) \in R$ tali che $(\bar{4}, \bar{8}) * (x, y) = (\bar{8}, \bar{4})$.

Esercizio 5. Sia M l'insieme dei polinomi monici di grado 3 in $\mathbb{Z}_3[x]$.

(*i*) Calcolare $|M|$.

Siano poi $A = \{f \in M \mid \bar{1} \text{ è radice di } f\}$ e $B = \{f \in M \mid \bar{1} \text{ e } \bar{2} \text{ sono radici di } f\}$.

(*ii*) Caratterizzare gli elementi di A e calcolare $|A|$.
(*iii*) Caratterizzare gli elementi di B e calcolare $|B|$.
(*iv*) È vero che ogni elemento di A è prodotto di tre polinomi irriducibili?
(*v*) È vero che ogni elemento di B è prodotto di tre polinomi irriducibili?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
21 MAGGIO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Si consideri l'applicazione $f\colon n \in \mathbb{N}^{\#} \longmapsto |D(n)| \in \mathbb{N}^{\#}$, dove, per ogni $n \in \mathbb{N}^{\#}$ si è posto $D(n) = \{a \in \mathbb{N} \,\big|\, a|n\}$.

(*i*) f è suriettiva?
(*ii*) f è iniettiva?

Sia $\mathcal{R}$ il nucleo di equivalenza di f. Allora:

(*iii*) Determinare gli elementi di $[1]_{\mathcal{R}}$, $[7]_{\mathcal{R}}$, $[6]_{\mathcal{R}}$;
(*iv*) Dire (giustificando in dettaglio le risposte) se le seguenti implicazioni sono vere o false per ogni $x, y \in \mathbb{N}^{\#}$:
  (a) $x < y \Rightarrow |D(x)| < |D(y)|$;
  (b) $|D(x)| < |D(y)| \Rightarrow x < y$;
  (c) $(x|y \wedge x \neq y) \Rightarrow |D(x)| < |D(y)|$.

Sia ora Σ la relazione d'ordine definita da: $(\forall x, y \in \mathbb{N}^{\#})\big(x\ \Sigma\ y \iff (f(x) < f(y) \vee x = y)\big)$.

(*v*) Σ è totale?
(*vi*) Quali sono gli elementi di $\mathbb{N}^{\#}$ che, rispetto a Σ, risultano confrontabili con ogni elemento di $\mathbb{N}^{\#}$?
(*vii*) $(\mathbb{N}^{\#}, \Sigma)$ ha minimo? Ha massimo?
(*viii*) Sia $X = \{1, 2, 3, 4, 5, 6\}$. (X, Σ) è un reticolo? Nel caso, è distributivo? È complementato?

Esercizio 2. Dare la definizione di *anello*; in quali casi un anello si dice *commutativo* o *unitario*?

Nell'insieme A delle applicazioni da $\mathbb{Z}_9$ a $\mathbb{Z}_9$ si definiscono le operazioni $+$ e $\cdot$ ponendo, per ogni f, $g \in A$,

$$f + g\colon x \in \mathbb{Z}_9 \mapsto f(x) + g(x) \in \mathbb{Z}_9; \qquad f \cdot g\colon x \in \mathbb{Z}_9 \mapsto f(x)g(x) \in \mathbb{Z}_9.$$

Risulta che $(A, +, \cdot)$ è un anello commutativo unitario (non è richiesta la verifica di questi fatti).

(*i*) Si determini in questo anello:
  (a) l'elemento neutro rispetto all'addizione;
  (b) l'opposto di un arbitrario elemento $f \in A$;
  (c) l'elemento neutro rispetto alla moltiplicazione;
  (d) l'insieme degli elementi invertibili.

Indicata, per ogni $a \in \mathbb{Z}_9$, con f_a l'applicazione costante $f_a\colon x \in \mathbb{Z}_9 \mapsto a \in \mathbb{Z}_9$,

(*ii*) si dimostri che $B := \{f_a \mid a \in \mathbb{Z}_9\}$ è una parte chiusa di $\mathbb{Z}_9$ rispetto a $+$ ed a $\cdot$;
(*iii*) si determini l'inverso in A di $f_{\bar{7}}$.

Esercizio 3. Per ogni primo p, sia f_p il polinomio $f_p = x^3 + x + \bar{4} \in \mathbb{Z}_p[x]$. Determinare i primi p tali che f_p sia divisibile per $x - \bar{2}$ in $\mathbb{Z}_p[x]$.

(*i*) Per ciascuno di tali primi, decomporre f_p in prodotto di polinomi irriducibili monici.
(*ii*) In $\mathbb{Z}_7[x]$, indicare, per ogni intero $n \in \mathbb{N}^{\#}$, un polinomio di grado $n + 1$ che sia prodotto di n polinomi irriducibili (non necessariamente distinti).

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
24 GIUGNO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di divisore e di multiplo di un elemento di $\mathbb{Z}$, e poi quello di massimo comun divisore tra due numeri interi. Elencare i divisori in $\mathbb{Z}$ di 28 e dire quanto valgono $\mathrm{MCD}(28,6)$ e $\mathrm{mcm}(28,6)$.

Esercizio 2. Per ogni numero intero $n>1$, indichiamo con f_n il massimo degli esponenti che appaiono nella decomposizione di n in prodotto di potenze di primi a due a due distinti. Più esplicitamente, se $n := p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_k^{\lambda_k}$, dove $p_1,\dots,p_k$ sono primi (positivi) tra loro distinti e $k,\lambda_1,\lambda_2,\dots,\lambda_k\in\mathbb{N}^{\#}$, poniamo $f_n=\max\{\lambda_1,\lambda_2,\dots,\lambda_k\}$. Posto $Y=\mathbb{N}\smallsetminus\{0,1\}$, sia f l'applicazione: $n\in Y\mapsto f_n\in\mathbb{N}^{\#}$.

(*i*) f è suriettiva?
(*ii*) f è iniettiva?

Sia $\mathcal{R}$ il nucleo di equivalenza di f. Allora:

(*iii*) Determinare gli elementi di $[30]_{\mathcal{R}}$ e di $[7]_{\mathcal{R}}$;
(*iv*) $[4]_{\mathcal{R}}$ è finito o infinito?
(*v*) $Y/\mathcal{R}$ è finito o infinito?

Sia ora Σ la relazione d'ordine definita in Y da: $(\forall x,y\in Y)\big(x\,\Sigma\,y\iff (f(x)<f(y)\vee x=y)\big)$.

(*vi*) Σ è totale?
(*vii*) (Y,Σ) ha minimo? Ha massimo? Descriverne gli eventuali elementi minimali o massimali.
(*viii*) Determinare minoranti, maggioranti, estremo inferiore ed estremo superiore di $\{49,88\}$ in (Y,Σ);
(*ix*) (Y,Σ) è un reticolo?

Posto $X=\{12,16,18,49,77,80\}$,

(*x*) Disegnare il diagramma di Hasse di (X,Σ).
(*xi*) Determinare eventuali elementi minimali, massimali, minimo, massimo in (X,Σ).
(*xii*) (X,Σ) è un reticolo?
(*xiii*) Determinare, se esiste, un elemento $a\in X$ tale che $(X\smallsetminus\{a\},\Sigma)$ sia un reticolo. Nel caso a esista, questo reticolo è distributivo? È complementato?

Esercizio 3. Per ogni intero positivo m, si definisca in $T_m:=\mathbb{Z}\times\mathbb{Z}_m$ un'operazione binaria $*$ come segue: per ogni $a,b\in\mathbb{Z}$ e $c,d\in\mathbb{Z}_m$, $(a,c)*(b,d)=(a+b-5,\bar{3}cd)$.

(*i*) Verificare che $(T_{14},*)$ è un monoide commutativo, indicandone l'elemento neutro.
(*ii*) Caratterizzare gli elementi simmetrizzabili di $(T_{14},*)$. Calcolare il simmetrico di $(9,\bar{9})$.
(*iii*) $\mathbb{Z}\times\{\bar{7}\}$ è una parte chiusa di $(T_{14},*)$?
(*iv*) Quali sono gli interi positivi m tali che $(T_m,*)$ sia un monoide?

Esercizio 4. Per ogni primo p, sia $f_p=30x^4+10x^3+11x^2+5x+4\in\mathbb{Z}_p[x]$. Determinare i primi p tali che f_p sia monico, di grado al più 3 e divisibile per x^2-1. Detto q il minimo tale primo, decomporre f_q nel prodotto di polinomi irriducibili monici.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
14 LUGLIO 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte.* Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Vero o falso? (E perché?)

(*i*) L'equazione congruenziale $24x \equiv_{128} 40$ ha soluzioni in $\mathbb{Z}$.
(*ii*) L'equazione congruenziale $24x \equiv_{128} 40$ ha esattamente una soluzione modulo 128.
(*iii*) Esistono $a, b \in \mathbb{Z}$ tali che $24a + 128b = 40$.
(*iv*) Per definizione, un anello commutativo è un dominio di integrità se e solo se tutti i suoi elementi diversi dallo zero sono invertibili.
(*v*) Posto $A = \{1, 4, 7, 10\}$ e $B = \{2, 5, 6\}$, si ha: $\{n \in \mathbb{N} \mid n \in A \Rightarrow n \in B\} = \varnothing$.

Esercizio 2. Nell'insieme $A = \{n \in \mathbb{N} \mid n < 9\}$ si consideri la relazione binaria $\sim$ definita da:

$$(\forall a, b \in A)(a \sim b \iff (a^2 \equiv_4 b^2 \ \wedge \ 10a + 1 \equiv_{15} 10b + 1)).$$

(*i*) Verificare che $\sim$ è una relazione di equivalenza.
(*ii*) Descrivere l'insieme quoziente $A/\!\sim$, elencando in modo esplicito gli elementi di ciascuna delle classi di equivalenza e calcolando $|A/\!\sim|$.

Esercizio 3. In $S := \mathbb{N} \times \{0, 1\}$ si definiscano le relazioni binarie ρ e σ:

$$(\forall (a, i), (b, j) \in S) \qquad \begin{array}{l} (a, i) \ \rho \ (b, j) \iff (a | b \wedge i \leq j); \\ (a, i) \ \sigma \ (b, j) \iff (a | b \vee i \leq j). \end{array}$$

(*i*) Spiegare perché ρ è una relazione d'ordine e perché σ non lo è.
(*ii*) (S, ρ) è un reticolo? Determinarne gli (eventuali) elementi minimali, massimali, minimo, massimo.
(*iii*) Descrivere l'insieme dei maggioranti di $A := \{(10, 0), (14, 0), (2, 1)\}$ in (S, ρ) e, se esiste, $\sup A$.

Posto $X = \{(1, 0), (2, 0), (2, 1), (4, 0), (6, 0), (10, 0), (100, 1)\}$,

(*iv*) Disegnare il diagramma di Hasse di (X, ρ). (X, ρ) è un reticolo?
(*v*) Determinare eventuali elementi minimali, massimali, minimo, massimo in (X, ρ).
(*vi*) Determinare, se esiste, un elemento $a \in S$ tale che $(X \cup \{a\}, \rho)$ sia un reticolo. È possibile scegliere a in modo che non sia il massimo di $(X \cup \{a\}, \rho)$? Nel caso a esista, il reticolo $(X \cup \{a\}, \rho)$ è distributivo? È complementato?

Esercizio 4. Sia $*$ l'operazione binaria definita in $\mathbb{Z}_{15}$ da: $(\forall a, b \in \mathbb{Z}_{15})(a * b = \bar{5}ab)$, e sia $+$ la consueta operazione di addizione $\mathbb{Z}_{15}$.

(*i*) Verificare che $(\mathbb{Z}_{15}, +, *)$ è un anello. È un anello commutativo? È unitario?
(*ii*) In $(\mathbb{Z}_{15}, +, *)$, quali tra $\bar{5}$, $\bar{3}$, $\bar{2}$ sono divisori dello zero?
(*iii*) Determinare tutti i divisori dello zero in $(\mathbb{Z}_{15}, +, *)$.

Esercizio 5. Si consideri il polinomio $f = 3x^4 - 2x^3 - 6x^2 + 6x - 20 \in \mathbb{Z}[x]$.

(*i*) Quali tra gli interi 1, 2, -1 sono radici di f?
(*ii*) In $\mathbb{Q}[x]$, decomporre f in prodotto di polinomi irriducibili.
(*iii*) Per ciascuno dei fattori irriducibili di f in $\mathbb{Q}[x]$ determinati al punto precedente, si dica se esso è o non è irriducibile in $\mathbb{R}[x]$.

(Si ricorda che è parte essenziale dell'esercizio la giustificazione del fatto che i fattori indicati come irriducibili lo siano effettivamente.)

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
5 SETTEMBRE 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte.* Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *partizione* di un insieme. Fornire esempi di partizioni $\mathcal{F}$ di $\mathbb{Z}$ tali che:

(*i*) $|\mathcal{F}| = 5$;
(*ii*) $\mathcal{F}$ sia un insieme infinito.

Esercizio 2. Esiste un $m \in \mathbb{N}^+$ tale che $\mathbb{Z}_m$ abbia esattamente 3 elementi invertibili e 7 divisori dello zero (viene escluso $[0]_m$)?

Esercizio 3. Siano $S = \{a, b\}$ e $T = \{0, 1\}$, dove $a \neq b$. Sia X l'insieme di tutte le applicazioni da S a T.

(*i*) Elencare gli elementi (applicazioni) di X.
(*ii*) Di ciascuna di queste applicazioni, dire se è iniettiva e se è suriettiva.

Definire in X la relazione binaria Σ ponendo, per ogni $f, g \in X$,

$$f \,\Sigma\, g \iff (\forall s \in S)(f(s) \leq g(s)).$$

(*iii*) Verificare che (X, Σ) è una relazione d'ordine.
(*iv*) (X, Σ) è totale?
(*v*) In (X, Σ) determinare, se esistono, minimo e massimo.
(*vi*) Disegnare il diagramma di Hasse di (X, Σ).
(*vii*) Esiste un insieme Y tale che (X, Σ) sia isomorfo a $(\mathcal{P}(Y), \subseteq)$?

Esercizio 4. Sia $*$ l'operazione binaria definita in $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$ da: $\forall a_1, b_1, a_2, b_2 \in \mathbb{Z}_{12}$,

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1).$$

(*i*) Verificare che $(\mathbb{Z}_{12} \times \mathbb{Z}_{12}, *)$ è un monoide, identificandone l'elemento neutro. Questo monoide è commutativo?
(*ii*) Determinare gli elementi invertibili di $(\mathbb{Z}_{12} \times \mathbb{Z}_{12}, *)$, descrivendone gli inversi;
(*iii*) calcolare in modo esplicito l'inverso di $(\bar{7}, \bar{2})$.

Esercizio 5. Detto S l'insieme dei polinomi di grado al più tre in $\mathbb{Z}_3[x]$, si considerino le applicazioni:

$$\varphi_1 \colon f \in S \mapsto f(\bar{1}) \in \mathbb{Z}_3 \qquad \text{e} \qquad \varphi_2 \colon f \in S \mapsto f(\bar{2}) \in \mathbb{Z}_3$$

(*i*) φ_1 è suriettiva? φ_2 è suriettiva?
(*ii*) Descrivere in modo esplicito le antiimmagini $A := \overleftarrow{\varphi_1}(\{\bar{0}\})$ e $B := \overleftarrow{\varphi_2}(\{\bar{0}\})$, e poi $A \cap B$, calcolando anche $|A|$, $|B|$ e $|A \cap B|$.
(*iii*) Stabilire se in A esistono polinomi che siano prodotto di due polinomi irriducibili.
(*iv*) Stabilire se in $A \cap B$ esistono polinomi che siano prodotto di due polinomi irriducibili.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
8 OTTOBRE 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *divisore* e di *multiplo* in $\mathbb{Z}$ di un numero intero a.
Posto, per ogni $a \in \mathbb{Z}$, $D(a) = \{n \in \mathbb{Z} \,\big|\, n|a\}$ e $M(a) = \{n \in \mathbb{Z} \,\big|\, a|n\}$,

(*i*) descrivere $D(11^{273})$;
(*ii*) esiste in $\mathbb{Z}$ un elemento a tale che $D(a)$ sia infinito?
(*iii*) Descrivere $\bigcap_{a\in\mathbb{Z}} D(a)$ e $\bigcup_{a\in\mathbb{Z}} D(a)$.

Definita la relazione binaria ρ in $\mathbb{Z}$, ponendo, per ogni $a, b \in \mathbb{Z}$, $\quad a \,\rho\, b \iff M(a) = M(b)$,

(*iv*) si spieghi perché ρ è una relazione di equivalenza;
(*v*) si descriva (in modo esplicito) la classe $[15]_\rho$.

Esercizio 2. Sia Σ la relazione binaria in $\mathbb{N}^+$ definita ponendo, per ogni $x, y \in \mathbb{N}^+$,

$$x \,\Sigma\, y \iff (\exists n \in \mathbb{N})(y = x2^n).$$

(*i*) Verificare che Σ è una relazione d'ordine.
(*ii*) Determinare, se esistono, gli elementi minimali, massimali, minimo, massimo in $(\mathbb{N}^+, \Sigma)$.
(*iii*) Verificare che, se $x, y \in \mathbb{N}^+$, avendo posto $x = k_x 2^{\alpha_x}$ e $y = k_y 2^{\alpha_y}$, dove $\alpha_x, \alpha_y \in \mathbb{N}$ mentre k_x e k_y sono interi positivi dispari, x e y sono confrontabili se e solo se $k_x = k_y$.
(*iv*) Verificare che, per ogni $x, y \in \mathbb{N}^+$, l'insieme $\{x, y\}$ ha maggioranti o minoranti se e solo se x e y sono confrontabili.
(*v*) Verificare che, per ogni $X \subseteq \mathbb{N}^+$, (X, Σ) è un reticolo se e solo se è totalmente ordinato.

Esercizio 3. Si definiscano in $S := \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ le operazioni binarie $*$ e $\oplus$ ponendo, per ogni $a, b, c, d, e, f \in \mathbb{Z}$,

$$(a, b, c) * (e, f, g) = (ae, af + bg, cg); \qquad (a, b, c) \oplus (e, f, g) = (a + e, b + f, c + g).$$

Dando per noto che $*$ è associativa,

(*i*) il semigruppo $(S, *)$ è un monoide? È commutativo?
(*ii*) Verificare che $(S, \oplus, *)$ è un anello. Di che tipo di anello si tratta?
(*iii*) $(1, -2, 0)$ è un divisore (destro?, sinistro?) dello zero in $(S, \oplus, *)$?
(*iv*) $(1, 0, 2)$ è invertibile in $(S, \oplus, *)$?

Esercizio 4. Determinare se esiste, o spiegare perché non esiste:

(*i*) un polinomio irriducibile di grado 3 in $\mathbb{Q}[x]$ che ammetta una radice in $\mathbb{Q}$;
(*ii*) un polinomio in $\mathbb{Q}[x]$ non irriducibile, che non ammetta radici in $\mathbb{Q}$;
(*iii*) un polinomio irriducibile di grado 3225 in $\mathbb{Q}[x]$;
(*iv*) un polinomio in $\mathbb{Q}[x]$, di grado 3225, che sia irriducibile sia in $\mathbb{Q}[x]$ che in $\mathbb{R}[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
12 NOVEMBRE 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte.* Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Con riferimento ad un insieme ordinato $(S, \leq)$, dare la definizione di minimo e di elemento minimale. Si forniscano esempi di:

(*i*) un reticolo complementato;
(*ii*) un reticolo privo di massimo e di minimo.

Esercizio 2. Sia $S = \{n \in \mathbb{N} \mid n < 8\}$ e si consideri l'applicazione

$$f\colon (X, Y) \in \mathcal{P}(S) \times \mathcal{P}(S) \mapsto |X \cap Y| \in \{n \in \mathbb{N} \mid n < 9\}$$

ed il suo nucleo di equivalenza $\sim_f$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Quanti sono gli $Y \in \mathcal{P}(S)$ tali che $f(\{4\}, Y) = 0$?
(*iii*) Quanti elementi ha $\mathcal{P}(S) \times \mathcal{P}(S)/\sim_f$? Esiste una coppia $(X, Y) \in \mathcal{P}(S) \times \mathcal{P}(S)$ tale che $[(X, Y)]_{\sim_f}$ abbia un solo elemento? Se sì, indicare una tale coppia.

Sia Σ la relazione d'ordine in $\mathcal{P}(S) \times \mathcal{P}(S)$ definita da: per ogni $X, Y, X', Y' \subseteq S$,

$$(X, Y)\ \Sigma\ (X', Y') \iff \big((X, Y) = (X', Y') \vee f(X, Y) < f(X', Y')\big).$$

(*iv*) Determinare, se esistono (o spiegare perché non esistono), gli elementi minimali, massimali, minimo, massimo in $(\mathcal{P}(S) \times \mathcal{P}(S), \Sigma)$.
(*v*) $(\mathcal{P}(S) \times \mathcal{P}(S), \Sigma)$ è un reticolo?
(*vi*) Determinare un sottoinsieme X di ordine 4 in $\mathcal{P}(S) \times \mathcal{P}(S)$ tale che (X, Σ) sia isomorfo a $(\mathcal{P}(\{1, 2\}), \subseteq)$.
(*vii*) Qual è la massima possibile cardinalità per una parte totalmente ordinata di $(\mathcal{P}(S) \times \mathcal{P}(S), \Sigma)$?

Esercizio 3. Si definisca in $S := \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z})$ l'operazione binaria $*$ ponendo, per ogni $A, A', B, B' \subseteq \mathbb{Z}$;

$$(A, B) * (A', B') = (A \triangle A', B \cup B').$$

(*i*) $*$ è commutativa? $*$ è associativa? Esiste in $(S, *)$ un elemento neutro?
(*ii*) Nel caso in cui esista elemento neutro, determinare gli elementi simmetrizzabili in $(S, *)$, descrivendone i simmetrici.
(*iii*) Che tipo di struttura è $(S, *)$ (un semigruppo, un monoide, un gruppo)?
(*iv*) Esiste $(X, Y) \in S$ tale che $(\mathbb{N}, \{1\}) * (X, Y) = (\{-1, 0, 1\}, \mathbb{N})$? Nel caso, tale coppia (X, Y) è univocamente determinata?
(*v*) Di ciascuna delle seguenti parti di S si dica se è chiusa rispetto a $*$, e per quelle chiuse si dica di che tipo di struttura si tratta:
  (a) $D := \{(X, X) \mid X \subseteq \mathbb{Z}\}$;
  (b) $Z_1 := \{(X, \varnothing) \mid X \subseteq \mathbb{Z}\}$;
  (c) $Z_2 := \{(\varnothing, X) \mid X \subseteq \mathbb{Z}\}$;

Esercizio 4. Il polinomio $f = x^4 - x^3 - \bar{3}x^2 + \bar{3}x - \bar{2} \in \mathbb{Z}_{11}[x]$ ha esattamente due radici in $\mathbb{Z}_{11}$. Di questa informazione, utile per lo svolgimento dell'esercizio, non è richiesta verifica. Trovare queste due radici, e poi scrivere f come prodotto di polinomi irriducibili monici.

Determinare tutte le coppie $(a, b) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ tali che $f + ax^4 + \bar{7}bx^3$ sia monico.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
10 DICEMBRE 2014

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *anello* e quella di *campo*. Ricordando di giustificare le risposte:

(*i*) $(\mathbb{N}, +, \cdot)$ è un anello?
(*ii*) Se S è un insieme, $(\mathcal{P}(S), \triangle, \smallsetminus)$ è un anello?
(*iii*) Se S è un insieme e $|S| > 1$, $(\mathcal{P}(S), \triangle, \cap)$ è un campo?

Dare un esempio di campo infinito ed uno di campo finito.

Esercizio 2. Si considerino le applicazioni

$$\varphi_3 \colon x \in \mathbb{Z}_{125} \mapsto \bar{3}x \in \mathbb{Z}_{125}; \qquad \text{e} \qquad \varphi_5 \colon x \in \mathbb{Z}_{125} \mapsto \bar{5}x \in \mathbb{Z}_{125}.$$

(*i*) φ_3 è iniettiva? φ_3 è suriettiva? φ_5 è iniettiva? φ_5 è suriettiva? Quale proprietà algebrica, che differenzia $\bar{3}$ e $\bar{5}$ in $\mathbb{Z}_{125}$, influisce sull'iniettività di φ_3 e φ_5?
(*ii*) Determinare gli interi positivi n tali che $\varphi_n \colon x \in \mathbb{Z}_{125} \mapsto \bar{n}x \in \mathbb{Z}_{125}$ sia biettiva.
(*iii*) Detto $\mathcal{R}_{\varphi_5}$ il nucleo di equivalenza di φ_5, descrivere esplicitamente $[\bar{0}]_{\mathcal{R}_{\varphi_5}}$, e calcolare le cardinalità di $[\bar{0}]_{\mathcal{R}_{\varphi_5}}$ e di $\vec{\varphi}_5(\mathbb{Z}_{125})$.

Esercizio 3. Si definisca in $\mathbb{Z}$ la relazione binaria Σ ponendo, per ogni $a, b \in \mathbb{Z}$:

$$a \,\Sigma\, b \iff (\exists h \in 2\mathbb{N})(a + h = b).$$

(*i*) Verificare che Σ è una relazione d'ordine e che non è totale.
(*ii*) Fissato $x \in 2\mathbb{Z}$, quali sono gli elementi $y \in \mathbb{Z}$ confrontabili con x? E se, invece, $x \in \mathbb{Z} \smallsetminus 2\mathbb{Z}$?
(*iii*) Determinare, se esistono (o spiegare perché non esistono), gli elementi minimali, massimali, minimo, massimo in $(\mathbb{Z}, \Sigma)$.
(*iv*) Dimostrare che, se X è una parte di $\mathbb{Z}$ tale che (X, Σ) sia un reticolo, (X, Σ) è necessariamente totalmente ordinato.

Esercizio 4. Si definisca in $\mathbb{Z} \times \mathbb{Z}$ l'operazione binaria $*$ ponendo, per ogni $a, b, c, d \in \mathbb{Z}$;

$$(a, b) * (c, d) = (a + c + 2, -bd).$$

Dando per noto (e quindi *non* verificando) che questa operazione è commutativa e associativa,

(*i*) determinare (se esiste) l'elemento neutro di $(\mathbb{Z} \times \mathbb{Z}, *)$. Nel caso, stabilire quali sono gli elementi simmetrizzabili, descrivendone i corrispondenti simmetrici;
(*ii*) determinare una parte infinita A di $\mathbb{Z} \times \mathbb{Z}$ che sia chiusa rispetto a $*$ e tale che $(A, *)$ sia un gruppo;
(*iii*) determinare una parte propria infinita B di $\mathbb{Z} \times \mathbb{Z}$ che sia chiusa rispetto a $*$ e tale che $(B, *)$ non sia un gruppo;
(*iv*) determinare una parte infinita C di $\mathbb{Z} \times \mathbb{Z}$ che non sia chiusa rispetto a $*$.

Esercizio 5. Per $p = 2$ e per $p = 7$ si consideri il polinomio $f_p := x^4 - \bar{2}x^3 + x^2 - \bar{1} \in \mathbb{Z}_p[x]$ e

(*i*) si scriva f_p come prodotto di polinomi irriducibili monici in $\mathbb{Z}_p[x]$.
(*ii*) Solo per $p = 7$, si costruisca l'associato monico $\tilde{g}$ di $g := \bar{4}x^4 - x^3 - \bar{3}x^2 - \bar{4}$ in $\mathbb{Z}_7[x]$. $\tilde{g}$ è associato a f_7?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
26 GENNAIO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. (*i*) Dare la definizione di *divisore* (in $\mathbb{Z}$) di un numero intero.
(*ii*) Per ogni $m \in \mathbb{Z}$ definire la relazione $\equiv_m$ di congruenza modulo m in $\mathbb{Z}$.
(*iii*) Per ogni $m, a \in \mathbb{Z}$ descrivere $[a]_{\equiv_m}$.
(*iv*) Determinare gli $m \in \mathbb{N}$ tali che $[27]_m = [-17]_m$.

Esercizio 2. Siano $\mathcal{P} = \mathcal{P}(\mathbb{N}) \setminus \{\varnothing\}$ e $\mathbb{P}$ l'insieme dei numeri primi positivi. Per ogni $X \in \mathcal{P}$, sia $\pi(X) = \{p \in \mathbb{P} \mid (\exists n \in X)(p|n)\}$. Consideriamo l'applicazione $f\colon X \in \mathcal{P} \mapsto \pi(X) \in \mathcal{P}(\mathbb{P})$ ed il suo nucleo di equivalenza $\mathcal{R}_f$.
(*i*) f è suriettiva? f è iniettiva?
(*ii*) Trovare un $\bar{Y} \in \mathcal{P}$ tale che $|[\bar{Y}]_{\mathcal{R}_f}| = 1$.
(*iii*) Verificare: $(\forall X \in \mathcal{P} \setminus \{\bar{Y}\})([X]_{\mathcal{R}_f}$ è infinito).
(*iv*) Caratterizzare gli $X \in \mathcal{P}$ tali che $|\pi(X)| = 1$.
(*v*) Dire, di ciascuna delle seguenti formule, se è vera o falsa (e perché):
(a) $(\forall X \in \mathcal{P})(X$ infinito $\Rightarrow \pi(X)$ infinito);
(b) $(\forall X \in \mathcal{P})(\pi(X)$ infinito $\Rightarrow X$ infinito);
(c) $(\forall X, Y \in \mathcal{P})(\pi(X) \cap \pi(Y) \neq \varnothing \Rightarrow X \cap Y \neq \varnothing)$;
(d) $(\forall X, Y \in \mathcal{P})(\pi(X) \cap \pi(Y) = \varnothing \Rightarrow X \cap Y = \varnothing)$;

Esercizio 3. Si definisca in $\mathbb{N}$ la relazione d'ordine Σ ponendo, per ogni $a, b \in \mathbb{N}$:

$$a \,\Sigma\, b \iff \big((a = b) \vee (\mathrm{rest}(a, 10) < \mathrm{rest}(b, 10) \wedge \mathrm{rest}(a, 5) < \mathrm{rest}(b, 5))\big).$$

(*i*) Stabilire se Σ è totale.
(*ii*) Determinare, se esistono (o spiegare perché non esistono), gli elementi minimali, massimali, minimo, massimo in $(\mathbb{N}, \Sigma)$.
(*iii*) Determinare l'insieme dei minoranti di $\{3, 7\}$ in $(\mathbb{N}, \Sigma)$. Esiste, in $(\mathbb{N}, \Sigma)$, $\inf\{3, 7\}$?
(*iv*) Posto $X = \{0, 1, 3, 6, 7, 9, 17\}$, si stabilisca se (X, Σ) è un reticolo.
(*v*) Di ciascuna delle seguenti parti di X di dica se, ordinata sempre da Σ, è un reticolo, un reticolo distributivo, un reticolo complementato: $X \setminus \{6\}$, $X \setminus \{7\}$, $X \setminus \{3\}$.

Esercizio 4. (*i*) Determinare gli $a \in \mathbb{Z}_7$ tali che il polinomio $x^2 - a$ sia irriducibile in $\mathbb{Z}_7[x]$.
(*ii*) Determinare il numero dei polinomi della forma $(x^2 - a)(x^2 - b) \in \mathbb{Z}_7[x]$, con $a, b \in \mathbb{Z}_7$, che siano:
(α) il prodotto di due polinomi irriducibili;
(β) il prodotto di tre polinomi irriducibili;
(γ) il prodotto di quattro polinomi irriducibili.

Esercizio 5. Sia $S = \{n \in \mathbb{N} \mid 1 \leq n \leq 10\}$. Sia $*$ l'operazione binaria definita in $\mathcal{P}(S)$ da:

$$(\forall X, Y \in \mathcal{P}(S))(X * Y = X \mathbin{\triangle} Y \mathbin{\triangle} \{1\}).$$

(*i*) $*$ è commutativa? $*$ è associativa?
(*ii*) determinare (se esiste) l'elemento neutro di $(\mathcal{P}(S), *)$. Nel caso, stabilire quali sono gli elementi simmetrizzabili, descrivendone i corrispondenti simmetrici.
(*iii*) Che tipo di struttura è $(\mathcal{P}(S), *)$?
(*iv*) Per ciascuna di $A := \{X \in \mathcal{P}(S) \mid 1 \in X\}$ e $B := \{X \in \mathcal{P}(S) \mid 1 \notin X\}$, si stabilisca se è una parte chiusa e, nel caso, se, munita dell'operazione indotta da $*$, è un gruppo.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 FEBBRAIO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Indicati con A un insieme non vuoto, con $\mathcal{R}$ una relazione di equivalenza in A e con a e b elementi di A,

- (i) definire la classe di equivalenza $[a]_{\mathcal{R}}$ e l'insieme quoziente $A/\mathcal{R}$;
- (ii) se $|A| = 10$, quali sono le possibili cardinalità per $A/\mathcal{R}$?
- (iii) Tra le seguenti, dire quali sono condizioni necessarie e sufficienti affinché $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$:
  (α) $a = b$; (β) $a \mathcal{R} b$; (γ) $[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}}$; (δ) $(\exists c \in A)(c \mathcal{R} a \wedge b \in [c]_{\mathcal{R}})$.

Esercizio 2. Sia $\mathcal{P} = \mathcal{P}(\mathbb{N}^+) \setminus \{\varnothing\}$ e sia φ l'applicazione: $X \in \mathcal{P} \longmapsto \{a + b \mid a, b \in X\} \in \mathcal{P}$.

- (i) Caratterizzare (se esistono) gli $X \in \mathcal{P}$ tali che:
  (α) $\varphi(X) = \{1\}$; (β) $|\varphi(X)| = 1$; (γ) $|\varphi(X)| = 2$.
- (ii) Calcolare $\varphi(\mathbb{N}^+)$ e $\varphi(\mathbb{N}^+ \setminus \{4\})$;
- (iii) φ è iniettiva? φ è suriettiva?
- (iv) Definita in $\mathcal{P}$ la relazione d'ordine Σ ponendo, per ogni $X, Y \in \mathcal{P}$,
$$X \,\Sigma\, Y \iff \big((X = Y) \vee (\varphi(X) \subset \varphi(Y))\big),$$
dire se Σ è totale e determinare in $(\mathcal{P}, \Sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo. $(\mathcal{P}, \Sigma)$ è un reticolo?
- (v) Posto $A = \big\{\{2\}, \{3\}, \{2,4\}, \{2,5\}, \{1,3,4,7\}\big\}$, disegnare il diagramma di Hasse di (A, Σ). Sempre in (A, Σ), determinare, se esistono, $\inf\big\{\{2,4\}, \{2,5\}\big\}$ e $\sup\big\{\{2,4\}, \{2,5\}\big\}$. (A, Σ) è un reticolo?
- (vi) Esiste $X \subseteq A$ tale che (X, Σ) sia un reticolo booleano di cardinalità 4?

Esercizio 3. Si consideri l'operazione binaria associativa $*$ definita in $\mathbb{Z}_8 \times \mathbb{Z}_8$ da:
$$(\forall a, b, c, d \in \mathbb{Z}_8)\big((a, b) * (c, d) = (ac, bc)\big).$$

- (i) Nel semigruppo $(\mathbb{Z}_8 \times \mathbb{Z}_8, *)$ si stabilisca se esistono elementi neutri a destra, neutri a sinistra, neutri.
- (ii) Sempre in $(\mathbb{Z}_8 \times \mathbb{Z}_8, *)$, si determinino le coppie (a, b) tali che
$$\big((a, b) * (\bar{4}, \bar{1}) = (\bar{0}, \bar{0})\big) \wedge \big((\bar{4}, \bar{1}) * (a, b) = (\bar{0}, \bar{0})\big).$$
- (iii) Verificare se $\mathbb{Z}_8 \times \{\bar{0}\}$ e $\{\bar{0}\} \times \mathbb{Z}_8$ sono parti chiuse rispetto a $*$. In caso di risposta affermativa studiare le strutture indotte (sono semigruppi, monoidi, gruppi? Sono commutative?).

Esercizio 4. (i) Trovare in $\mathbb{Z}_7[x]$, se ne esistono, polinomi:

- (α) f, di grado 7, che abbia 7 radici distinte in $\mathbb{Z}_7$;
- (β) g, di grado 7, che sia il prodotto di 7 fattori irriducbili ed abbia esattamente una radice in $\mathbb{Z}_7$;
- (γ) h, di grado 7, che sia il prodotto di 7 fattori irriducbili e non abbia radici in $\mathbb{Z}_7$.

- (ii) Scomporre, in $\mathbb{Z}_7[x]$, $x^4 - \bar{4}$ in prodotto di fattori irriducibili monici.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
5 MARZO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *anello booleano* e fornirne due esempi, uno finito ed uno infinito.

Esercizio 2. Posto $S = \{1, 2, 3, 4\}$, si verifichi che la relazione binaria $\sim$, definita in $\mathcal{P}(S)$ da:

$$\big(\forall X, Y \in \mathcal{P}(S)\big)\big(X \sim Y \iff \big((2 \in X \iff 2 \in Y) \wedge (\{1,3\} \subseteq X \iff \{1,3\} \subseteq Y)\big)\big)$$

è una relazione di equivalenza.

(*i*) Elencare gli elementi di $[S]_\sim$.
(*ii*) Dire quanti elementi ha $\mathcal{P}(S)/\sim$, senza calcolare esplicitamente le classi.
(*iii*) Elencare gli elementi di $[\varnothing]_\sim$.

Se cambiamo la definizione di $\sim$, sostituendo "$(2 \in X \iff 2 \in Y)$" con "$(2 \notin X \iff 2 \notin Y)$", otteniamo ancora una relazione di equivalenza? Cosa cambia?

Esercizio 3. Definamo l'applicazione $\varphi\colon \mathbb{N}^* \smallsetminus \{1\} \to \mathbb{N}^*$ in questo modo: per ogni $n \in \mathbb{N}^* \smallsetminus \{1\}$, scritto n come prodotto di primi nella forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, dove $r \in \mathbb{N}^*$, i p_i sono numeri primi positivi tra loro distinti e, per ogni $i \in \{1, 2, \dots, r\}$, $\alpha_i \in \mathbb{N}^*$, poniamo $\varphi(n) = \alpha_1 \alpha_2 \cdots \alpha_r$.

(*i*) Spiegare perché l'applicazione φ è ben definita (da quale teorema dipende questo fatto?).
(*ii*) φ è iniettiva? φ è suriettiva?
(*iii*) Descrivere le antiimmagini $\overleftarrow{\varphi}(\{1\})$, $\overleftarrow{\varphi}(\{2\})$, $\overleftarrow{\varphi}(\{4\})$ e $\overleftarrow{\varphi}(\{p\})$ per un arbitrario numero primo p.
(*iv*) Verificare che, detto $\mathcal{R}$ il nucleo di equivalenza di φ, per ogni numero primo p, in ciascuna classe di equivalenza modulo $\mathcal{R}$ esiste una ed una sola potenza di p;

Definiamo ora in $\mathbb{N}^* \smallsetminus \{1\}$ la relazione d'ordine σ ponendo, per ogni $a, b \in \mathbb{N}^* \smallsetminus \{1\}$,

$$a \,\sigma\, b \iff \big((a = b) \vee (\varphi(a) < \varphi(b))\big).$$

(*v*) Stabilire se σ è totale.
(*vi*) Vero o falso (e perché?): se $a, b \in \mathbb{N}^* \smallsetminus \{1\}$ e $\varphi(a) \neq \varphi(b)$ allora a e b sono confrontabili rispetto a σ.
(*vii*) Determinare, se possibile, un sottoinsieme X di $\mathbb{N}^* \smallsetminus \{1\}$ tale che:
(a) $|X| = 6$ e (X, σ) sia totalmente ordinato;
(b) $|X| = 6$ e (X, σ) sia un reticolo non distributivo;
(c) $|X| = 6$ e (X, σ) sia un reticolo distributivo non totalmente ordinato;
(d) $|X| = 6$ e (X, σ) sia un reticolo distributivo e complementato;
(e) $|X| = 8$ e (X, σ) sia un reticolo distributivo e complementato.

Esercizio 4. Per quali $k \in \mathbb{Z}_{17}$ il polinomio $f_k = \bar{5}kx^3 + (\bar{3}k + \bar{2})x^2 + \overline{11}kx + \bar{6}k \in \mathbb{Z}_{17}[x]$ ammette $\bar{1}$ come radice? (Si usi una equazione congruenziale). Scelto uno di questi valori, si fattorizzi f_k come prodotto di polinomi irriducibili in $\mathbb{Z}_{17}[x]$.

Esercizio 5. Si dica quanti elementi ha $S := \mathbb{Z}_8^* \times \mathbb{Z}_8$ (dove $\mathbb{Z}_8^* = \mathcal{U}(\mathbb{Z}_8)$). Si consideri l'operazione binaria $*$ definita in S da:

$$(\forall (a, b), (c, d) \in S)\big((a, b) * (c, d) = (ac, ad + b)\big).$$

(*i*) Che tipo di struttura è $(S, *)$? (Semigruppo, monoide, gruppo? Commutativo?).
(*ii*) Di ciascuna di $T = \mathbb{Z}_8^* \times \mathbb{Z}_8^*$ e $U = \mathbb{Z}_8^* \times (\mathbb{Z}_8 \smallsetminus \mathbb{Z}_8^*)$ si dica se è una parte chiusa di $(S, *)$ e, nel caso, che tipo di struttura sia la quella indotta.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
18 MAGGIO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *anello* e quella di *divisore dello zero* in un anello. Fornire poi un esempio di divisore dello zero (non nullo) in un anello ed un esempio di anello privo di divisori dello zero non nulli.

Esercizio 2. Per ogni $n \in \mathbb{N}$, sia $D^*(n)$ l'insieme dei divisori propri di n in $\mathbb{N}$ (ad esempio, $D^*(6) = \{1, 2, 3\}$). Posto $S = \mathbb{N}^* \smallsetminus \{1\}$, consideriamo l'applicazione $\varphi\colon n \in S \mapsto \max D^*(n) \in \mathbb{N}^*$.

(*i*) φ è iniettiva? φ è suriettiva?
(*ii*) Calcolare l'immagine $\vec{\varphi}(\{n \in \mathbb{N} \mid 1 < n < 10\})$ e l'antiimmagine $\overleftarrow{\varphi}(\{5\})$.

Sia $\mathcal{R}$ il nucleo di equivalenza di φ e sia $\mathcal{R}'$ il nucleo di equivalenza della restrizione di φ a $X := \{n \in \mathbb{N} \mid 1 < n < 10\}$.

(*iii*) Descrivere le classi $[5]_{\mathcal{R}}$ e $[10]_{\mathcal{R}}$ in $S/\mathcal{R}$.
(*iv*) Quanti elementi ha $X/\mathcal{R}'$? Descrivere $[6]_{\mathcal{R}'}$.

Sia Σ la relazione d'ordine definita in S da: $\quad (\forall a, b \in S)\big(a \,\Sigma\, b \iff (a = b \ \vee\ 2\varphi(a) \mid \varphi(b)\big)$.

(*v*) Determinare gli elementi minimali e gli elementi massimali in (S, Σ).

Posto $A = \{4, 8, 12, 17, 24, 40, 1200\}$,

(*vi*) si disegni il diagramma di Hasse di (A, Σ).
(*vii*) (A, Σ) è un reticolo? Nel caso, è distributivo? È complementato?
(*viii*) Determinare, se esiste, un $a \in A$ tale che $(A \smallsetminus \{a\}, \Sigma)$ sia un reticolo distributivo.
(*ix*) Determinare, se esiste, un $n \in S$ tale che $(A \cup \{n\}, \Sigma)$ sia un reticolo booleano.

Esercizio 3. Si consideri, nell'insieme $\mathbb{Z}_{15}$, l'operazione binaria $*$ definita ponendo $a*b = \bar{6}(a+b) - \bar{5}ab$ per ogni $a, b \in \mathbb{Z}_{15}$.

(*i*) Si stabilisca se $*$ è commutativa e se è associativa.
(*ii*) Determinare $a \in \mathbb{Z}_{15}$ tale che $a * \bar{1} = \bar{1}$ e stabilire se tale a è un elemento neutro di $(\mathbb{Z}_{15}, *)$.
(*iii*) Che tipo di struttura è $(\mathbb{Z}_{15}, *)$?
(*iv*) Si trovi, in $(\mathbb{Z}_{15}, *)$, una parte chiusa di cardinalità 2 (suggerimento, si parta dall'elemento $\bar{5}$).
(*v*) Se la domanda ha senso, si elenchino gli elementi simmetrizzabili in $(\mathbb{Z}_{15}, *)$ (suggerimento: assegnato $a \in \mathbb{Z}$, il MCD positivo d tra $6 - 5a$ e 15 è uno tra 1 e 3 (perché?). Se $d = 1$, $\bar{a}$ è simmetrizzabile in $(\mathbb{Z}_{15}, *)$? E se $d = 3$?)

Esercizio 4. Si trovi un primo p tale che il polinomio $f = \bar{3}x^4 + x^3 + x + \bar{2} \in \mathbb{Z}_p[x]$ sia divisibile, in $\mathbb{Z}_p[x]$, per $x^2 + 1$. Quanti di tali primi p esistono? Per il fissato primo p,

(*i*) Si scomponga f come prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.
(*ii*) Quanti sono i polinomi associati a f in $\mathbb{Z}_p[x]$? Se possibile, se ne scriva uno monico.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
22 GIUGNO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *partizione* di un insieme A. Supposto poi $|A| = 5$:

(*i*) qual è la cardinalità minima possibile per una partizione di A? E qual è la cardinalità massima possibile per una partizione di A?
(*ii*) Quante sono le partizioni di A costituite da due elementi, uno di ordine 2 ed uno di ordine 3?

Esercizio 2. Sia $S = \{a, b, c\}$, un insieme di cardinalità 3, e sia $T = \mathcal{P}(S) \times \mathcal{P}(S)$. Si consideri l'applicazione

$$f\colon (X, Y) \in T \longmapsto |X| \cdot |Y| \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Detto $\mathcal{R}$ il nucleo di equivalenza di f, determinare $|T/\mathcal{R}|$, $|[(\{a\}, \{b\})]_{\mathcal{R}}|$, $|[(\varnothing, \{a, b\})]_{\mathcal{R}}|$ e $|[(S, S)]_{\mathcal{R}}|$.

Considerata in T la relazione d'ordine Σ definita ponendo, per ogni $(X, Y), (Z, R) \in T$,

$$(X, Y)\ \Sigma\ (Z, R) \iff \big((X, Y) = (Z, R) \vee |X| \cdot |Y| < |Z| \cdot |R|\big),$$

(*iii*) determinare gli elementi minimali, massimali e gli eventuali minimo e massimo in (T, Σ).
(*iv*) (T, Σ) è un reticolo?

Sia $L = \{A, B, C, D, E, F, G, H\} \subseteq T$, dove

$$A = (\varnothing, S), \quad B = (\{a\}, \{b\}), \quad C = (\{b\}, \{a\}), \quad D = (\{a\}, \{b, c\}),$$
$$E = (\{a, b\}, \{c\}), \quad F = (\{a, b\}, \{a\}), \quad G = (\{a, b\}, \{a, b\}), \quad H = (\{a, c\}, S).$$

(*v*) Disegnare il diagramma di Hasse di (L, Σ).
(*vi*) (L, Σ) non è un reticolo. Perché?
(*vii*) Qual è il minimo numero di elementi da eliminare da L per ottenere:
  (α) un reticolo;
  (β) un reticolo distributivo;
  (γ) un reticolo booleano.

Esercizio 3. Nell'insieme $M = \mathbb{Z}_8 \times \mathbb{Z}_8$ si consideri l'operazione binaria $*$ definita ponendo, per ogni $a, b, c, d \in \mathbb{Z}_8$,

$$(a, b) * (c, d) = (a + c + \bar{2}, \bar{3}bd).$$

(*i*) Verificare che $(M, *)$ è un semigruppo commutativo. Stabilire se è un monoide (studiando un'opportuna equazione congruenziale) e, nel caso, determinarne gli elementi invertibili.
(*ii*) Verificare che $K := \{(\overline{2h}, \overline{2k}) \mid h, k \in \mathbb{Z}\}$ è una parte chiusa in $(M, *)$.
(*iii*) Spiegare perché, se $h, t \in \mathbb{Z}$ e t è dispari, non si può avere $\overline{2h} = \bar{t}$; calcolare $|K|$.
(*iv*) Caratterizzare gli interi $m > 1$ tali che l'operazione $\bullet$, definita in $\mathbb{Z}_m \times \mathbb{Z}_m$ ponendo $(a, b) \bullet (c, d) = (a + c + \bar{2}, \bar{3}bd)$ per ogni $a, b, c, d \in \mathbb{Z}_m$, non ammetta elemento neutro.

Esercizio 4.

(*i*) Sia $f = x^2 + ax + b$ un polinomio (monico) irriducibile in $\mathbb{Z}_3[x]$. Spiegare perché, necessariamente, $b \neq \bar{0}$.
(*ii*) Si elenchino i polinomi monici di grado due irriducibili in $\mathbb{Z}_3[x]$.
(*iii*) Si descrivano (*senza fare calcoli ulteriori*) i polinomi monici di grado quattro in $\mathbb{Z}_3[x]$ che non abbiano radici in $\mathbb{Z}_3$ e non siano irriducibili in $\mathbb{Z}_3[x]$. Quanti ne sono?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
13 LUGLIO 2015

Svolgere i seguenti esercizi, *giustificando* ***pienamente*** *tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia. Dopo aver letto queste righe alzare le braccia in segno di assenso.

Esercizio 1. (*i*) Dare la definizione di *divisore* di un numero n in $\mathbb{Z}$.
(*ii*) L'insieme $\{[-8]_5, [8]_5, [19]_5, [55]_5, [76]_5, [103]_5\}$ coincide con $\mathbb{Z}_5$?
(*iii*) Per quali interi $n > 1$ si ha $[15]_8 = [n]_8$?

Esercizio 2. Si consideri l'applicazione $f\colon (a,b) \in \mathbb{N}\times\mathbb{N} \mapsto a^2+b^2 \in \mathbb{N}$.
(*i*) f è iniettiva? f è suriettiva?
(*ii*) Detto $\mathcal{R}$ il nucleo di equivalenza di f, elencare gli elementi di $[(4,3)]_{\mathcal{R}}$ e calcolare $|[(4,3)]_{\mathcal{R}}|$.
(*iii*) La relazione binaria τ definita in $\mathbb{N}\times\mathbb{N}$ da:

$$(\forall a,b,c,d \in \mathbb{N})\big((a,b)\ \tau\ (c,d) \iff f(a,b) \le f(c,d)\big)$$

non è d'ordine. Perché?

Sia invece σ la relazione d'ordine in $\mathbb{N}\times\mathbb{N}$ definita da:

$$(\forall a,b,c,d \in \mathbb{N})\big((a,b)\ \sigma\ (c,d) \iff ((a,b)=(c,d) \vee f(a,b) < f(c,d))\big)$$

(*iv*) σ è totale?
(*v*) È vero che, scelti comunque $a,b,c,d \in \mathbb{N}$, se $(a,b) \neq (c,d)$ allora (a,b) e (c,d) sono confrontabili rispetto a σ?
(*vi*) Determinare gli elementi minimali, massimali e gli eventuali minimo e massimo in $(\mathbb{N}\times\mathbb{N},\sigma)$.
(*vii*) Posto $A = \{(1,0),(0,1)\}$, determinare in $(\mathbb{N}\times\mathbb{N},\sigma)$ l'insieme dei minoranti e quello dei maggioranti di A e, se esistono, $\inf A$ e $\sup A$. Rispondere alla stessa domanda dopo aver sostituito A con $B = \{(1,4),(4,1)\}$.
(*viii*) $(\mathbb{N}\times\mathbb{N},\sigma)$ è un reticolo?

Sia $X = \{(0,4),(1,3),(1,4),(2,3),(3,1),(4,1),(4,2)\}$.
(*ix*) Disegnare il diagramma di Hasse di (X,σ). (X,σ) è un reticolo?
(*x*) Qual è il minimo numero di elementi da eliminare da X per ottenere (rispetto all'ordinamento indotto da σ):
(α) un reticolo;
(β) un reticolo distributivo;
(γ) un reticolo complementato.
(*xi*) Esiste $x \in \mathbb{N}\times\mathbb{N}$ tale che $(X\cup\{x\},\sigma)$ sia un reticolo? Se la risposta è sì, il reticolo così ottenuto è complementato? Quanti sono gli $x \in \mathbb{N}\times\mathbb{N}$ con la proprietà richiesta?

Esercizio 3. Si consideri in $\mathbb{Z}_9$ l'operazione binaria $*$ definita ponendo, $a*b = a+b+\bar{6}ab$ per ogni $a,b \in \mathbb{Z}_9$.
(*i*) Stabilire che tipo di struttura è $(\mathbb{Z}_9,*)$: un semigruppo?, commutativo o no?, un monoide? un gruppo? un anello?
(*ii*) Nel caso in cui la domanda abbia senso, $\bar{2}$ è simmetrizzabile in $(\mathbb{Z}_9,*)$? Se sì, calcolarne il simmetrico.
(*iii*) Stabilire se $\{\bar{0},\bar{2}\}$ è una parte chiusa in $(\mathbb{Z}_9,*)$.

Esercizio 4. Per ogni $a \in \mathbb{Z}_5$, sia f_a il polinomio $x^3 - x + a \in \mathbb{Z}_5[x]$.
(*i*) Per quali (e quanti) valori di $a \in \mathbb{Z}_5$ il polinomio f_a *non* è irriducibile?
(*ii*) Scelto un tale a, che sia diverso da $\bar{0}$, si decomponga f_a in prodotto di polinomi monici irriducibili in $\mathbb{Z}_5[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
7 SETTEMBRE 2015

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome, cognome, matricola*** *e* ***gruppo di appartenenza***. Non è necessario consegnare la traccia.

Esercizio 1. Si dia la definizione di *grafo* (semplice) e quella di *grafo connesso*.

Esercizio 2. Indicato con $\mathbb{P}$ l'insieme degli interi positivi primi, e posto $X = \{10, 25, 26\}$, elencare gli elementi di ciascuno degli insiemi:

$A = \{p \in \mathbb{P} \mid (\forall x \in X)(p|x)\}$,
$B = \{p \in \mathbb{P} \mid (\exists x \in X)(x|p)\}$,
$C = \{p \in \mathbb{P} \mid (\forall x \in X)(p|x \vee p < x)\}$,
$D = \{p \in \mathbb{P} \mid p < 20 \wedge (\forall x \in X)(p|x \Rightarrow p = 2)\}$,
$E = \{p \in \mathbb{P} \mid p > 8 \Rightarrow (\exists x \in X)(p|x)\}$.

Esercizio 3. Nell'insieme $S = \{1, 2, 3\}$ si consideri la relazione binaria α di grafico

$$\{(1,1), (1,3), (2,2), (3,1), (3,3)\}.$$

α una relazione di equivalenza? Nel caso lo sia, elencare le classi di equivalenza in S/α.

Esercizio 4. Si considerino le relazioni binarie $\mathcal{S}$ e $\mathcal{R}$ definite in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$,

$$a \,\mathcal{S}\, b \iff (a \leq b \vee \mathrm{rest}(a,3) \mid \mathrm{rest}(b,3)); \qquad a \,\mathcal{R}\, b \iff (a \leq b \wedge \mathrm{rest}(a,3) \mid \mathrm{rest}(b,3)).$$

(*i*) $\mathcal{S}$ non è né d'ordine né di equivalenza; perché?
(*ii*) Invece $\mathcal{R}$ è d'ordine. Determinare gli eventuali elementi minimali, massimali, minimo e massimo in $(\mathbb{N}, \mathcal{R})$.
(*iii*) Quali dei seguenti sono reticoli, e quali no? Per quelli che lo sono, specificare se sono reticoli distributivi e se sono reticoli complementati: $(\mathbb{N}, \mathcal{R})$, $(3\mathbb{N}+1, \mathcal{R})$, $(A, \mathcal{R})$, $(B, \mathcal{R})$, dove $A = \{n \in \mathbb{N} \mid n \leq 9\}$ e $B = \{1, 7, 18, 23, 31, 300\}$. Nel rispondere, disegnare i diagrammi di Hasse di $(A, \mathcal{R})$ e $(B, \mathcal{R})$.
(*iv*) In $(\mathbb{N}, \mathcal{R})$, determinare, se esistono, $\inf\{59, 61\}$ e $\sup\{59, 61\}$.
(*v*) Spiegare perché non esistono in $(\mathbb{N}, \mathcal{R})$ quattro elementi a due a due non confrontabili tra loro.

Esercizio 5. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12} \mapsto ab \in \mathbb{Z}_{12}$.

(*i*) f è suriettiva?
(*ii*) Determinare gli elementi dell'insieme $A = \{a \in \mathbb{Z}_{12} \mid (\exists b \in \mathbb{Z}_{12} \smallsetminus \{\bar{0}\})((a,b) \in \overleftarrow{f}(\{\bar{0}\}))\}$.
(*iii*) Determinare gli elementi dell'insieme $B = \{a \in \mathbb{Z}_{12} \mid (\exists b \in \mathbb{Z}_{12})((a,b) \in \overleftarrow{f}(\{\bar{1}\}))\}$.
(*iv*) $\mathcal{F} := \{A, B\}$ è una partizione di $\mathbb{Z}_{12}$? (Giustificare la risposta in tutti i dettagli).
(*v*) Indicata, per ogni $a \in \mathbb{Z}_{12}$, con f_a l'applicazione: $b \in \mathbb{Z}_{12} \mapsto ab \in \mathbb{Z}_{12}$, dire per quali $a \in \mathbb{Z}_{12}$ f_a è iniettiva e per quali f_a è suriettiva.
(*vi*) Determinare, se possibile, l'applicazione inversa di $f_{\bar{7}}$ (utilizzare e risolvere a questo scopo un'opportuna equazione congruenziale).

Esercizio 6.

(*i*) Senza effettuare prodotti, si spieghi perché in $\mathbb{Z}_5[x]$ si ha $x^5 - x = x(x-\bar{1})(x-\bar{2})(x-\bar{3})(x-\bar{4})$.
(*ii*) Si costruisca un polinomio $g \in \mathbb{Z}_5[x]$ di grado 5 che non ammetta radici in $\mathbb{Z}_5$.

Per ogni primo p, sia f_p il polinomio $x^5 - x \in \mathbb{Z}_p[x]$.

(*iii*) Per ogni p, si giustifichi il fatto che f_p è prodotto, in $\mathbb{Z}_p[x]$, di fattori di grado 1 se e solo se $x^2 + \bar{1}$ ha radici in $\mathbb{Z}_p$
(*iv*) Si trovi un primo p tale che f_p abbia, in $\mathbb{Z}_p[x]$, un fattore irriducibile di grado 2.
(*v*) Esiste un primo p tale che f_p abbia, in $\mathbb{Z}_p[x]$, un fattore irriducibile di grado 3?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 OTTOBRE 2015

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome, cognome, matricola*** *e* ***gruppo di appartenenza***. Non è necessario consegnare la traccia.

Esercizio 1. Si dia la definizione di *anello*. Si dia poi la definizione di anello *booleano* e se ne fornisca un esempio.

Esercizio 2. Sia $X = \{n \in \mathbb{N} \mid n < 5\}$, per ogni $n \in \mathbb{Z}$, sia $\pi(n)$ l'insieme dei divisori primi positivi di n. Si consideri la relazione binaria $\sim$ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \sim b \iff \pi(a) \cap X = \pi(b) \cap X.$$

Stabilire se $\sim$ è una relazione di equivalenza. Nel caso lo sia,

(*i*) calcolare $|\mathbb{Z}/\!\sim|$;
(*ii*) posto $A = \{n \in \mathbb{Z} \mid -5 \leq n \leq 10\}$, elencare gli elementi di ciascuna classe in $A/\!\sim$ e calcolare $|A/\!\sim|$.

Ripetere l'esercizio per la relazione binaria σ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \,\sigma\, b \iff \pi(a) \cap X = (\pi(b) \cap X) \cup \{5\}.$$

Esercizio 3. Sia

$$*\colon (X, Y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \longmapsto \begin{cases} \varnothing; & \text{se } X \cup Y = \varnothing \\ \{\min(X \cup Y)\}; & \text{se } X \cup Y \neq \varnothing \end{cases} \in \mathcal{P}(\mathbb{N}).$$

(*i*) Spiegare perché $*$ è ben definita (lo sarebbe se sostituissimo $\mathbb{Z}$ ad $\mathbb{N}$ nella sua definizione?).
(*ii*) $*$ è iniettiva? È suriettiva? Calcolare l'immagine $\operatorname{im} *$ dell'applicazione $*$ e l'antiimmagine $\overleftarrow{*}(\{\{0\}, \{1\}\})$ dell'insieme $\{\{0\}, \{1\}\}$.
(*iii*) Che genere di struttura algebrica è $(\mathcal{P}(\mathbb{N}), *)$ (semigruppo, monoide, gruppo; commutativo o no)?
(*iv*) Determinare, se esiste, $X \in \mathcal{P}(\mathbb{N})$ tale che, $(\forall Y \in \mathcal{P}(\mathbb{N}))(X * Y = X)$. Quanti tali X esistono?
(*v*) $\mathcal{P}_1(\mathbb{N}) = \{\{n\} \mid n \in \mathbb{N}\}$ è una parte chiusa in $(\mathcal{P}(\mathbb{N}), *)$? Se lo è, che genere di struttura algebrica è $(\mathcal{P}_1(\mathbb{N}), *)$? Rispondere alle stessa domande dopo aver sostituito $\mathcal{P}_1(\mathbb{N})$ con $\mathcal{P}_2(\mathbb{N}) = \{X \subset \mathbb{N} \mid |X| = 2\}$.

Esercizio 4.

(*i*) Di ciascuno degli insiemi $P = 2\mathbb{N}$, $D = 2\mathbb{N} + 1$, $X = \{n \in \mathbb{N} \mid n < 100\}$, $Y = X \smallsetminus \{0\}$ si dica se, ordinato dalla relazione di divisibilità (in $\mathbb{N}$) è o non è sottoreticolo di $(\mathbb{N}, |)$, se ha minimo, se ha massimo.

Sia poi $S = \{0, 1, 2, 4, 6, 10, 36, 60\}$.

(*ii*) Disegnare il diagramma di Hasse di S ordinato per divisibilità. Questo è un reticolo?
(*iii*) Determinare un elemento $a \in S$ tale che $T = S \smallsetminus \{a\}$, ordinato per divisibilità, sia un reticolo.
(*iv*) Disegnare il diagramma di Hasse del reticolo T determinato al punto precedente e stabilire se T è totalmente ordinato, distributivo, complementato, booleano.

Esercizio 5. Per ogni $\lambda \in \mathbb{Z}_{11}$ sia f_λ il polinomio

$$x^4 + \bar{6}\lambda x^3 + \lambda x^2 + \bar{6}x + \bar{3} \in \mathbb{Z}_{11}[x].$$

(*i*) Stabilire per quali valori di λ il polinomio f_λ è divisibile per $(x + \bar{1})^2$ in $\mathbb{Z}_{11}[x]$;
(*ii*) Fissato uno di questi valori per λ, scrivere f_λ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_{11}[x]$. Suggerimento: per il passaggio finale è utile elencare i quadrati degli elementi di $\mathbb{Z}_{11}$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
16 NOVEMBRE 2015

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome***, ***cognome***, ***matricola*** *e* ***gruppo di appartenenza***. Non è necessario consegnare la traccia.

Esercizio 1. Si diano le definizioni di *applicazione iniettiva* e di *applicazione suriettiva*. Posto $X = \{n \in \mathbb{N} \mid n < 10\}$, si fornisca (o si spieghi perché non esiste) un esempio di:

(*i*) un'applicazione iniettiva non suriettiva $f\colon \mathbb{N} \to \mathbb{N}$;
(*ii*) un'applicazione suriettiva non iniettiva $g\colon \mathbb{N} \to \mathbb{N}$;
(*iii*) un'applicazione iniettiva non suriettiva $h\colon X \to X$;
(*iv*) un'applicazione suriettiva non iniettiva $k\colon X \to X$.

Esercizio 2.

(*i*) Si disegni il diagramma di Hasse dell'insieme $\{n \in \mathbb{N} \mid n < 9\}$ ordinato per divisibilità.

Considerata la relazione d'ordine σ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a \,\sigma\, b \iff \big(a = b \text{ oppure } \operatorname{rest}(a, 9) \text{ è un divisore proprio di } \operatorname{rest}(b, 9)\big),$$

(*ii*) determinare gli (eventuali) elementi minimali, massimali, minimo, massimo in $(\mathbb{Z}, \sigma)$;
(*iii*) stabilire se $(\mathbb{Z}, \sigma)$ è un reticolo;
(*iv*) decidere se in $(\mathbb{Z}, \sigma)$ esiste una catena infinita.

Sia $A = \{2, 5, 10, 13, 18, 20, 22, 40, 50\}$.

(*v*) Disegnare il diagramma di Hasse di (A, σ);
(*vi*) stabilire se (A, σ) è un reticolo;
(*vii*) trovare $x \in A$ tale che $(A \smallsetminus \{x\}, \sigma)$ sia un reticolo e decidere se questo reticolo è distributivo, complementato, booleano (si ricorda che le risposte vanno giustificate in modo esauriente).

Esercizio 3. In $T = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$ si definisca l'operazione binaria $*$ ponendo, per ogni $a, b, c, x, y, z \in \mathbb{Z}_{10}$,

$$(a, b, c) * (x, y, z) = (ax, ay + bz, cz).$$

(*i*) Sapendo che $*$ è associativa (non è richiesta verifica di questo fatto), dimostrare che $(T, *)$ è un monoide e che non è commutativo.

Sia $K = \{(a, b, c) \in T \mid a, c \in \mathcal{U}(\mathbb{Z}_{10})\}$;

(*ii*) calcolare $|K|$;
(*iii*) verificare che K è una parte chiusa rispetto a $*$;
(*iv*) verificare che $(K, *)$ è un gruppo;
(*v*) calcolare l'inverso in $(K, *)$ di $(\overline{7}, \overline{5}, \overline{7})$, svolgendo *una* equazione congruenziale utilizzando l'algoritmo euclideo.

Esercizio 4. Per ogni primo (positivo) p, sia f_p il polinomio

$$\overline{65}x^5 + \overline{10}x^4 + \overline{11}x^3 + \overline{5}x^2 + \overline{7}x + \overline{12} \in \mathbb{Z}_p[x].$$

(*i*) Trovare un primo q tale che f_q sia monico di grado 5 (quanti ce ne sono?).
(*ii*) Trovare un primo r tale che f_r sia monico di grado 3 (quanti ce ne sono?).
(*iii*) Decomporre f_q come prodotto di polinomi monici irriducibili in $\mathbb{Z}_q[x]$.
(*iv*) Decomporre f_r come prodotto di polinomi monici irriducibili in $\mathbb{Z}_r[x]$.
(*v*) f_r ha in $\mathbb{Z}_r[x]$ un divisore irriducibile di coefficiente (parametro) direttore $\overline{2}$?
(*vi*) f_r ha in $\mathbb{Z}_r[x]$ un divisore irriducibile di grado 2?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
14 DICEMBRE 2015

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome, cognome, matricola*** *e* ***gruppo di appartenenza***. Non è necessario consegnare la traccia. Buone feste.

Esercizio 1.

(*i*) Scrivere gli elementi invertibili ed i divisori dello zero (diversi dallo zero) dell'anello $\mathbb{Z}_{10}$.
(*ii*) Esiste un intero positivo m tale che in $\mathbb{Z}_m$ esistano esattamente 7 elementi invertibili e 3 divisori dello zero (diversi dallo zero)?
(*iii*) Sia A un anello unitario con $1_A \neq 0_A$. È possibile che tutti gli elementi di $A \setminus \{0_A\}$ siano divisori dello zero?

Esercizio 2. Sia $\overline{\mathbb{N}} = \mathbb{N} \setminus 10\mathbb{N}$. Per ogni $x \in \overline{\mathbb{N}}$ indichiamo con $\alpha(x)$ il numero ottenuto da x invertendo l'ordine delle sue cifre (nella rappresentazione in base 10; ad esempio $\alpha(1273) = 3721$). Si consideri l'applicazione

$$\alpha\colon x \in \overline{\mathbb{N}} \longmapsto \alpha(x) \in \mathbb{N}.$$

(*i*) α è iniettiva? α è suriettiva?
(*ii*) Quanti sono gli $x \in \overline{\mathbb{N}}$ di tre cifre fissati da α (cioè tali che $\alpha(x) = x$)?

Si definisca in $\overline{\mathbb{N}}$ la relazione d'ordine σ ponendo, per ogni $x, y \in \overline{\mathbb{N}}$,

$$x \,\sigma\, y \iff (x \leq y \wedge \alpha(x) \leq \alpha(y)).$$

(*iii*) σ è totale?
(*iv*) Si determinino rispetto a σ, se esistono, $\min \overline{\mathbb{N}}$, $\max \overline{\mathbb{N}}$, gli elementi minimali, gli elementi massimali.
(*v*) Provare che, per ogni $x, y \in \overline{\mathbb{N}}$:
  (a) se il numero delle cifre di x è minore di quello di y, allora $x \,\sigma\, y$;
  (b) se $x - 1 \in \overline{\mathbb{N}}$, allora $(x-1) \,\sigma\, x$.
(*vi*) Calcolare in $(\overline{\mathbb{N}}, \sigma)$ i minoranti e l'estremo inferiore di $\{14, 22\}$.
(*vii*) Posto $X = \{11, 16, 23, 27, 35, 37\}$, disegnare il diagramma di Hasse di (X, σ). Trovare, se possibile un $h \in \overline{\mathbb{N}}$ tale che $(X \cup \{h\}, \sigma)$ sia un reticolo.

Esercizio 3. In $R = \mathbb{Z}_5 \times \mathbb{Z}_5$ si definiscano le operazioni binarie $\oplus$ e $*$ ponendo, per ogni $a, b, x, y \in \mathbb{Z}_5$,

$$(a,b) \oplus (x,y) = (a+x, b+y); \qquad (a,b) * (x,y) = (ax - by, ay + bx).$$

(*i*) Tenendo presente che $\oplus$ e $*$ sono associative e commutative (queste proprietà non vanno verificate), provare che $(R, \oplus, *)$ è un anello commutativo.
(*ii*) Trovare tutti gli $s \in R$ tali che $(\bar{0}, \bar{1}) * s = (\bar{0}, \bar{1})$.
(*iii*) $(R, \oplus, *)$ è unitario?
(*iv*) Per ciascuno degli elementi $(\bar{0}, \bar{1})$ e $(\bar{1}, \bar{2})$ di R dire se si tratta di un divisore dello zero e se è invertibile (nel caso, specificando l'inverso).
(*v*) $(R, \oplus, *)$ è un dominio di integrità? È un campo?
(*vi*) $A := \mathbb{Z}_5 \times \{\bar{0}\}$ è una parte chiusa di R rispetto a $\oplus$? E rispetto a $*$? Nel caso entrambe le risposte siano positive: $(A, \oplus, *)$ è un campo?

Esercizio 4. Per ogni primo (positivo) p ed ogni $\lambda \in \mathbb{Z}_p$, sia $f_{p,\lambda}$ il polinomio

$$\overline{10}\lambda(x^3 + \lambda + \overline{29})^{1000} \in \mathbb{Z}_p[x].$$

Per ciascuno dei primi p in $\{2, 3, 5, 7, 97\}$, trovare, se possibile, $\lambda \in \mathbb{Z}_p$ tale che $f_{p,\lambda}$ sia monico (eseguire l'algoritmo euclideo solo per il caso $p = 97$) e, se un tale λ è stato trovato, scrivere $f_{p,\lambda}$ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
22 GENNAIO 2016

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome, cognome, matricola*** *e* ***gruppo di appartenenza***. Non è necessario consegnare la traccia.

Esercizio 1. Assegnati tre interi a, b, m, con $m \neq 0$, si consideri l'equazione congruenziale

$$ax \equiv_m b. \qquad (*)$$

(*i*) Cosa significa dire che l'intero u è soluzione di $(*)$?
(*ii*) Fornire una condizione necessaria e sufficiente affinché $(*)$ abbia almeno una soluzione in $\mathbb{Z}$.
(*iii*) Se $u \in \mathbb{Z}$ è una soluzione di $(*)$, come si può descrivere, in generale, l'insieme di *tutte* le soluzioni di $(*)$ in $\mathbb{Z}$?

Esercizio 2. Per ogni intero positivo n, indichiamo con $C(n)$ la somma delle cifre di n (quando n sia scritto in base 10. Ad esempio, $C(3049) = 3+0+4+9 = 16$). Consideriamo la relazione d'ordine σ definita in $S := \{n \in \mathbb{N} \mid 1 \leq n \leq 100001\}$ ponendo, per ogni $a, b \in S$,

$$a \,\sigma\, b \iff (a = b \vee C(a) < C(b)).$$

(*i*) Si determinino in (S, σ), gli eventuali elementi minimali, massimali, minimo, massimo.
(*ii*) σ è totale?
(*iii*) (S, σ) è un reticolo?
(*iv*) Disegnare il diagramma di Hasse di (T, σ), dove $T = \{5, 21, 32, 44, 101, 771, 906, 2000, 11111\}$. (T, σ) è un reticolo?
(*v*) Determinare, se possibile (o spiegare perché non esiste) una parte K di T tale che $|K| = 5$ e (K, σ) sia un reticolo distributivo non totalmente ordinato.

Esercizio 3. Per ogni polinomio $f \in \mathbb{Z}_5[x]$, sia $R(f) = \{a \in \mathbb{Z}_5 \mid f(a) = \bar{0}\}$, l'insieme delle radici di f in $\mathbb{Z}_5$.

(*i*) Determinare (o spiegare perché non esiste) un $f \in \mathbb{Z}_5[x]$ tale che $R(f) = \{\bar{1}, \bar{3}\}$.
(*ii*) Verificare che per ogni $X \subseteq \mathbb{Z}_5$ esiste $f \in \mathbb{Z}_5[x]$ tale che $R(f) = X$.

Sia ora F l'applicazione $f \in \mathbb{Z}_5[x] \longmapsto R(f) \in \mathcal{P}(\mathbb{Z}_5)$.

(*iii*) F è iniettiva? F è suriettiva?

Detta poi $\sim$ la relazione binaria definita in $\mathbb{Z}_5[x]$ ponendo, per ogni $f, g \in \mathbb{Z}_5[x]$, $f \sim g \iff R(f) = R(g)$,

(*iv*) spiegare perché $\sim$ è una relazione di equivalenza;
(*v*) decidere se $\bar{1} \sim x^2 + \bar{2}$ e se $\bar{1} \sim (x^2 + \bar{2})^{500}$;
(*vi*) calcolare $|\mathbb{Z}_5[x]/\!\sim|$.
(*vii*) Esiste $f \in \mathbb{Z}_5[x]$ tale che $[f]_\sim$ sia finito?

Esercizio 4. Considerare, in $M := \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$, l'operazione binaria $*$ definita da:

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, a_1b_2 + b_1c_2, c_1c_2)$$

per ogni $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}_{10}$.

(*i*) $*$ è associativa? È commutativa?
(*ii*) $(M, *)$ ha elemento neutro?
(*iii*) Descrivere l'insieme degli elementi invertibili in $(M, *)$, specificandone anche gli inversi.
(*iv*) Stabilire se, in $(M, *)$, l'elemento $(\bar{3}, \bar{5}, \bar{3})$ ha inverso, e nel caso calcolare questo inverso.
(*v*) Spiegare perché, scelti comunque $u, v \in \mathbb{Z}$, se $u \equiv_{10} v$, allora si ha: u è pari se e solo se v è pari.
(*vi*) Posto $D = \{\bar{b} \in \mathbb{Z}_{10} \mid b \text{ è un intero dispari}\}$ e $P = \{\bar{b} \in \mathbb{Z}_{10} \mid b \text{ è un intero pari}\}$, per ciascuna delle parti $A := \mathbb{Z}_{10} \times D \times \mathbb{Z}_{10}$ e $B := \mathbb{Z}_{10} \times P \times \mathbb{Z}_{10}$ si dica se è o meno chiusa in $(M, *)$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
18 FEBBRAIO 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza.* Non è necessario consegnare la traccia.

Esercizio 1. Fornire la definizione di partizione, quella di relazione di equivalenza ed enunciare un teorema che leghi, per un fissato insieme A, le relazioni di equivalenza in A con le partizioni di A.

Se A è un insieme di 1000 elementi, quante sono le partizioni $\{X, Y\}$ di A tali che $|X| = 999$?

Esercizio 2. Si consideri l'applicazione

$$\varphi\colon (a,b) \in \mathbb{N}^* \times \mathbb{N}^* \longmapsto ab+1 \in \mathbb{N}^*$$

(*i*) φ è iniettiva? φ è suriettiva?
(*ii*) Determinare $\overleftarrow{\varphi}(\{7\})$ e, se p e q sono primi distinti, $|\overleftarrow{\varphi}(\{pq+1\})|$ e $|\overleftarrow{\varphi}(\{p^2+1\})|$.
(*iii*) Caratterizzare gli $x \in \mathbb{N}^*$ tali che $|\overleftarrow{\varphi}(\{x\})| = 2$.
(*iv*) Esiste $x \in \mathbb{N}^*$ tale che $|\overleftarrow{\varphi}(\{x\})| = 1$?

Sia ora Σ la relazione d'ordine in $\mathbb{N}^* \times \mathbb{N}^*$ definita da: per ogni $a, b, c, d \in \mathbb{N}^*$,

$$(a,b)\ \Sigma\ (c,d) \iff \big((a,b) = (c,d) \vee \varphi((a,b)) < \varphi((c,d))\big).$$

(*v*) Σ è totale?
(*vi*) Si determinino in $(\mathbb{N}^* \times \mathbb{N}^*, \Sigma)$, gli eventuali elementi minimali, massimali, minimo, massimo.
(*vii*) Sia $X = \{(1,2),(2,1)\}$. Determinare, in $(\mathbb{N}^* \times \mathbb{N}^*, \Sigma)$, gli insiemi dei minoranti e dei maggioranti di X e, se esistono, $\inf X$ e $\sup X$.
(*viii*) $(\mathbb{N}^* \times \mathbb{N}^*, \Sigma)$ è un reticolo?
(*ix*) Determinare, se possibile, sottoinsiemi Y e Z di $\mathbb{N}^* \times \mathbb{N}^*$ tali che (Y, Σ) sia un reticolo isomorfo al reticolo trirettangolo M_3 e (Z, Σ) sia un reticolo isomorfo a $(\mathcal{P}(\{1,2,3\}, \subseteq)$. (Suggerimento: disegnare il diagramma di Hasse di quest'ultimo).

Esercizio 3. Considerare, in $\mathbb{Z}_{50}$, l'operazione binaria $*$ definita da $a * b = \bar{4}ab$ per ogni $a, b \in \mathbb{Z}_{50}$.

(*i*) $*$ è commutativa? È associativa?
(*ii*) $(\mathbb{Z}_{50}, *)$ ha elemento neutro?
(*iii*) Provare che $P = \{\bar{2}\bar{k} \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}_{50}$ è una parte chiusa in $(\mathbb{Z}_{50}, *)$.
(*iv*) Esiste $k \in \mathbb{Z}$ tale che $\bar{2} = \bar{2} * \bar{k}$?
(*v*) Stabilire se, in $(P, *)$, esiste elemento neutro. In caso di risposta positiva,
  (a) trovare l'eventuale inverso di $\bar{2}$ in $(P, *)$;
  (b) provare che, per ogni $k \in \mathbb{Z}$, $\bar{2}\bar{k}$ è invertibile in $(P, *)$ se e solo se 5 non divide k in $\mathbb{Z}$.
(*vi*) Determinare una parte chiusa Q di P tale che $(Q, *)$ sia un gruppo.

Esercizio 4. Sia S l'insieme dei polinomi di grado al più 3 in $\mathbb{Z}_3[x]$. Considerata l'applicazione $\psi\colon a_0 + a_1x + a_2x^2 + a_3x^3 \in S \mapsto a_1 + \bar{2}a_2x + \bar{3}a_3x^2 \in \mathbb{Z}_3[x]$,

(*i*) descrivere $A := \{f \in S \mid \psi(f) = \bar{0}\}$; calcolare $|A|$;
(*ii*) descrivere $B := \operatorname{im}\psi = \vec{\psi}(S)$; calcolare $|B|$;
(*iii*) verificare che, per ogni $f \in S$, se $(x-\bar{1})^2$ divide f, allora $x - \bar{1}$ divide $\psi(f)$.
(*iv*) Determinare un polinomio $f \in \mathbb{Z}_3[x]$ di grado 2 e privo di radici in $\mathbb{Z}_3$. Il polinomio $g = f \cdot f$ è irriducibile in $\mathbb{Z}_3[x]$?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
10 MARZO 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza.* Non è necessario consegnare la traccia.

Esercizio 1. Dare le definizioni di *grafo*, di *grafo connesso* e di *albero*. In $V := \{-2, -1, 1, 2\}$, la relazione binaria τ definita da $x \ \tau \ y \iff xy < 0$ per ogni $x, y \in V$ definisce un grafo? In caso di risposta positiva, tale grafo è connesso? È un albero?

Esercizio 2. Sia X l'insieme delle applicazioni di $S := \{1, 2, 3\}$ in sé.

(*i*) Calcolare $|X|$.
(*ii*) Quante sono, tra le applicazioni in X, quelle iniettive? E quante le suriettive?

Definiamo ora la relazione binaria σ in X ponendo, per ogni $f, g \in X$,

$$f \ \sigma \ g \iff \big((\forall i \in S)(f(i) \leq g(i))\big).$$

(*iii*) Costruire un'applicazione non costante $h \in X$ tale che $\mathrm{id}_S \ \sigma \ h$, dove id_S è l'applicazione identica: $i \in S \mapsto i \in S$.
(*iv*) σ è una relazione d'ordine? Se lo è rispondere alle domande che seguono.
(*v*) σ è totale?
(*vi*) Esistono in (X, σ) massimo e minimo?
(*vii*) Per ogni f e g, sia $\ell_{f,g} \colon i \in S \mapsto \min\{f(i), g(i)\} \in S$. Allora:
  (a) $\ell_{f,g}$ è un minorante di $\{f, g\}$ in (X, σ)?
  (b) se lo è, è il massimo tra questi minoranti?
(*viii*) (X, σ) è un reticolo?
(*ix*) (X, σ) è un reticolo booleano?

Esercizio 3. Si consideri in $\mathcal{P}(\mathbb{Z}_{24})$, l'operazione binaria $*$ definita ponendo, per ogni $A, B \in \mathcal{P}(\mathbb{Z}_{24})$,

$$A * B = \{ab \mid a \in A \wedge b \in B\}$$

(*i*) $*$ è commutativa? È associativa?
(*ii*) Esiste in $(\mathcal{P}(Z_{24}), *)$ elemento neutro?
(*iii*) Nel caso elemento neutro esista, caratterizzare in $(\mathcal{P}(\mathbb{Z}_{24}), *)$ gli elementi invertibili, descrivendone gli inversi.
(*iv*) Vale per ogni $A, B \in \mathcal{P}(\mathbb{Z}_{24})$ l'equivalenza: $A * B = \{\bar{0}\} \iff (A = \{\bar{0}\} \vee B = \{\bar{0}\})$?
(*v*) Determinare gli $A \in \mathcal{P}(\mathbb{Z}_{24})$ tali che $\{\bar{7}\} * A = \{\bar{7}, \bar{1}\}$ (utilizzare una opportuna equazione congruenziale).
(*vi*) $\{\bar{7}, \bar{1}\}$ è cancellabile in $(\mathcal{P}(\mathbb{Z}_{24}), *)$?

Esercizio 4. Sia α la relazione binaria in $\mathbb{Z}_7[x]$ definita da:

$$(\forall f, g \in \mathbb{Z}_7[x])(f \ \alpha \ g \iff x - \bar{1} \mid f - g).$$

(*i*) α è una relazione di equivalenza?
(*ii*) Verificare che, per ogni $f, g \in \mathbb{Z}_7[x]$, si ha: $f \ \alpha \ g \iff f(\bar{1}) = g(\bar{1})$.
(*iii*) Se α è di equivalenza:
  (a) descrivere le classi di equivalenza rispetto a α, scegliendo un rappresentante per ciascuna di esse e calcolando $|\mathbb{Z}_7[x]/\alpha|$;
  (b) per ogni $n \in \mathbb{N}$ e per ogni $f \in \mathbb{Z}_7[x]$ costruire, se possibile, un rappresentante di $[f]_\alpha$ di grado n.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
13 MAGGIO 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza.* Non è necessario consegnare la traccia.

Esercizio 1.

(*i*) Per ogni intero positivo k, dare un esempio di relazione di equivalenza in $\mathbb{Z}$ che determini esattamente k classi di equivalenza.
(*ii*) Scrivere tutte le partizioni dell'insieme $\{1, 2, 3\}$.
(*iii*) Dare un esempio di anello di cardinalità 8 con esattamente 6 divisori dello zero non nulli.

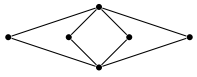
Esercizio 2. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{N} \times \mathbb{N} \longmapsto a + b \in \mathbb{N}$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Indicato con $\mathcal{R}_f$ il nucleo di equivalenza di f, descrivere $[(1, 4)]_{\mathcal{R}_f}$. Più in generale, considerato un arbitrario $(a, b) \in \mathbb{N} \times \mathbb{N}$ e posto $n = a + b$, quanti e quali sono gli elementi di $[(a, b)]_{\mathcal{R}_f}$?

Sia Σ la relazione d'ordine definita in $\mathbb{N} \times \mathbb{N}$ ponendo, per ogni $a, b, c, d \in \mathbb{N}$,

$$(a, b)\ \Sigma\ (c, d) \iff \big((a, b) = (c, d) \vee a + b < c + d\big).$$

(*iii*) Σ è totale? Più in generale, se $(a, b) \in \mathbb{N} \times \mathbb{N}$, quali sono gli elementi di $\mathbb{N} \times \mathbb{N}$ con cui (a, b) è confrontabile?
(*iv*) Determinare, se esistono, in $(\mathbb{N} \times \mathbb{N}, \Sigma)$, maggioranti, minoranti, estremo inferiore ed estremo superiore di $\{(1, 3), (5, 2)\}$ e di $\{(1, 3), (2, 2)\}$.
(*v*) Verificare che, per ogni $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, esiste $\sup\{(a, b), (c, d)\}$ (in $(\mathbb{N} \times \mathbb{N}, \Sigma)$) se e solo se (a, b) e (c, d) sono tra loro confrontabili.
(*vi*) Determinare un sottoinsieme X di $\mathbb{N} \times \mathbb{N}$ tale che (X, Σ) abbia come diagramma di Hasse quello qui disegnato:



Esercizio 3. Si provi che $F := \left\{ \left(\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right) \;\middle|\; a \in \mathbb{R} \right\}$ è una parte chiusa in $M_2(\mathbb{R})$ sia rispetto all'addizione tra matrici che rispetto al prodotto righe per colonne. Ricordando che le proprietà di associatività, commutatività e distributività si ereditano da un anello alle sue parti chiuse, dimostrare che F, munito delle operazioni di addizione e prodotto righe per colonne tra matrici, è un campo.

Esercizio 4. Costruire ove possibile:

(*i*) un polinomio f_1 di grado 5 irriducibile in $\mathbb{Q}[x]$;
(*ii*) un polinomio f_2 di grado 5 irriducibile in $\mathbb{Q}[x]$ che sia il prodotto di due polinomi in $\mathbb{Q}[x]$, uno di grado 2 ed uno di grado 3;
(*iii*) un polinomio f_3 di grado 5 che sia il prodotto di due polinomi irriducibili in $\mathbb{Q}[x]$;
(*iv*) un polinomio f_4 di grado 5 irriducibile in $\mathbb{R}[x]$;
(*v*) un polinomio f_5 di grado 5 che sia il prodotto di tre polinomi irriducibili in $\mathbb{R}[x]$;
(*vi*) un polinomio f_6 di grado 5 in $\mathbb{R}[x]$ che sia privo di radici in $\mathbb{R}$;
(*vii*) un polinomio f_7 di grado 5 che sia il prodotto di cinque polinomi irriducibili in $\mathbb{R}[x]$ e che abbia esattamente una radice in $\mathbb{R}$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
20 GIUGNO 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* Non è necessario consegnare la traccia.

Esercizio 1. Per ogni $x \in \mathbb{N}^* \smallsetminus \{1\}$, scritto x nella forma

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

dove $t \in \mathbb{N}^*$, $p_1, p_2, \ldots, p_t$ sono primi positivi a due a due distinti tra loro, $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{N}^*$, poniamo:

$$\alpha_x = \alpha_1 + \alpha_2 + \cdots + \alpha_t; \qquad \beta_x = p_1 p_2 \cdots p_t; \qquad p_x = \min\{p \in \mathbb{P} \mid p \text{ divide } x\}$$

(dove $\mathbb{P}$ è l'insieme dei numeri interi positivi primi). Posto $X = \{15, 54, 100\}$, si determinino:

$$A = \{\alpha_x \mid x \in X\}; \qquad B = \{\beta_x \mid x \in X\}; \qquad C = \left\{ \frac{x}{p_x} \;\middle|\; x \in X \right\}.$$

Esercizio 2. Sia $\mathbb{P}$ l'insieme dei numeri interi positivi primi e si ponga $S = \mathbb{N}^* \smallsetminus \{1\}$. Per ogni $n \in S$, siano $\pi(n)$ l'insieme dei primi in $\mathbb{P}$ che dividono n, $p_n = \min \pi(n)$ e $q_n = \max \pi(n)$. Si consideri poi l'applicazione $f\colon n \in S \longmapsto (p_n, q_n) \in \mathbb{P} \times \mathbb{P}$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Si determini $\vec{f}(S)$.
(*iii*) Si caratterizzino gli $n \in S$ per i quali esista $p \in \mathbb{P}$ tale che $f(n) = (p, p)$.
(*iv*) Detto $\mathcal{R}_f$il nucleo di equivalenza di f, si elenchino gli elementi di $[4]_{\mathcal{R}_f} \cap \{a \in S \mid a \leq 20\}$.

Sia Σ la relazione binaria definita in S da:

$$(\forall n, m \in S) \quad \big(n \,\Sigma\, m \iff \big(n = m \vee (p_n | p_m \wedge q_n < q_m)\big)\big).$$

(*v*) Si verifichi che Σ è una relazione d'ordine e che non è totale.
(*vi*) Si determinino in (S, Σ) gli eventuali elementi minimali, massimali, minimo, massimo.
(*vii*) (S, Σ) è un reticolo?
(*viii*) Si determini, per ogni $n \in S$, l'insieme degli elementi di S confrontabili con n rispetto a Σ.
(*ix*) Verificare che esiste un sottoinsieme X di S tale che $|X| = 4$ e (X, Σ) sia un reticolo non totalmente ordinato.

Esercizio 3. (*i*) Elencare gli elementi del gruppo $(\mathcal{U}(\mathbb{Z}_9), \cdot)$ degli invertibili di $\mathbb{Z}_9$.

Nel prodotto cartesiano $G = \mathbb{Z}_9 \times \mathcal{U}(\mathbb{Z}_9)$, si definisca l'operazione binaria $*$ ponendo:

$$(\forall\, (a, b), (c, d) \in G)\ \big((a, b) * (c, d) = (a + c + \bar{3}, \bar{2}bd)\big).$$

(*ii*) Si provi che $(G, *)$ è un gruppo.
(*iii*) Determinare l'inverso di $(\bar{2}, \bar{7})$ in $(G, *)$.
(*iv*) Dire, di ciascuna delle parti $X := \big(\mathbb{Z}_9 \smallsetminus \mathcal{U}(\mathbb{Z}_9)\big) \times \{\bar{4}, \bar{5}\}$ e $Y := \mathbb{Z}_9 \times \{\bar{2}, \bar{5}\}$, se è o non è chiusa di $(G, *)$.

Esercizio 4.

(*i*) Si determinino i primi (positivi) p per i quali il polinomio $f_p = x^3 - \overline{7}x^2 + \overline{14}x + \overline{24} \in \mathbb{Z}_p[x]$ sia divisibile per $x + \bar{2}$.
(*ii*) Per ciascuno dei primi p così determinati, si decomponga f_p in prodotto di polinomi irriducibili in $\mathbb{Z}_p[x]$.
(*iii*) Per gli stessi primi p, quanti sono in $\mathbb{Z}_p[x]$ i polinomi associati a f_p?
(*iv*) Il polinomio $f = x^3 - 7x^2 + 14x + 24 \in \mathbb{R}[x]$ ha in $\mathbb{R}$ almeno una radice?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
11 LUGLIO 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* Non è necessario consegnare la traccia.

Esercizio 1.

(*i*) Dare la definizione di *divisore* e di *multiplo* in $\mathbb{Z}$ di un numero intero.
(*ii*) Per un intero m, definire la relazione di *congruenza modulo* m in $\mathbb{Z}$, ...
(*iii*) ...e descrivere, per un arbitrario $a \in \mathbb{Z}$, $[a]_m$.
(*iv*) Determinare gli $m \in \mathbb{N}$ per i quali:
(α): $[3]_m = [21]_m$; (β): $[3]_m = [-3]_m$; (γ): $[3]_m = [3]_m^{-1}$;

Esercizio 2. Per ogni intero positivo m si definisca l'operazione binaria $*_m$ in $\mathbb{Z}_m$ ponendo, per ogni $a, b \in \mathbb{Z}_m$,

$$a *_m b = \overline{10}a + \overline{6}b.$$

(*i*) Dopo aver calcolato $\bar{1} *_m \bar{0}$, $\bar{0} *_m \bar{1}$, $(\bar{0} *_m \bar{0}) *_m \bar{1}$, $\bar{0} *_m (\bar{0} *_m \bar{1})$, caratterizzare gli $m \in \mathbb{N}^*$ tali che:
(α) $*_m$ sia commutativa;
(β) $*_m$ sia associativa;
(γ) $*_m$ sia associativa e commutativa.
(*ii*) Determinare tutti e soli gli $a \in \mathbb{Z}_{34}$ tali che $a *_{34} \bar{1} = \bar{0}$. Stabilire se $\bar{1}$ è cancellabile in $(\mathbb{Z}_{34}, *_{34})$.

Sia ora m il massimo intero positivo tale che $*_m$ sia associativa e poniamo $* = *_m$.

(*iii*) Decidere se $(\mathbb{Z}_m, *)$ ha elementi neutri a destra e/o a sinistra e, nel caso, descriverli *[Suggerimento: si trovino gli $a \in \mathbb{Z}_m$ tali che $a * \bar{0} = \bar{0}$].*
(*iv*) Sia $X = \{\bar{6}n \mid n \in \mathbb{Z}_m\}$. X è una parte chiusa in $(\mathbb{Z}_m, *)$? Se lo è, decidere se $(X, *)$ ha elementi neutri a destra e/o a sinistra e, nel caso, descriverli.

Esercizio 3. Consideriamo la funzione resto, $f\colon (a, b) \in \mathbb{N} \times \mathbb{N}^* \longmapsto \mathrm{rest}(a, b) \in \mathbb{N}$. Sia $\mathcal{R}$ il suo nucleo di equivalenza.

(*i*) f è suriettiva?
(*ii*) La restrizione di f a $\mathbb{N} \times \{1000\}$ è iniettiva?
(*iii*) La restrizione di f a $\{1000\} \times \mathbb{N}^*$ è iniettiva?
(*iv*) Descrivere $[(4, 2)]_{\mathcal{R}}$.

Sia ora Σ la relazione d'ordine definita in $S := \mathbb{N} \times \mathbb{N}^*$ ponendo, per ogni $a, c \in \mathbb{N}$ e $b, d \in \mathbb{N}^*$:

$$(a, b)\ \Sigma\ (c, d) \iff \big((a, b) = (c, d) \vee f((a, b)) \text{ è un divisore proprio di } f((c, d))\big).$$

(*v*) Si determinino in (S, Σ) gli eventuali elementi minimali, massimali, minimo, massimo. (S, Σ) è un reticolo?
(*vi*) Si determini l'insieme dei minoranti in (S, Σ) dell'insieme $X := \{8, 15\} \times \{4, 5\}$. Decidere se esiste (e, nel caso, individuare) $\inf_{(S,\Sigma)} X$.
(*vii*) Esibire se esiste, o provare che non esiste, un sottoinsieme Y di S tale che (Y, Σ) sia un reticolo pentagonale.

Esercizio 4. Per ogni intero primo p, sia $f_p = x^3 - x + \bar{1} \in \mathbb{Z}_p[x]$.

(*i*) Determinare il minimo primo positivo $\bar{p}$ tale che $f_{\bar{p}}$ *non* sia irriducibile in $\mathbb{Z}_{\bar{p}}[x]$;
(*ii*) scrivere $f_{\bar{p}}$ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_{\bar{p}}[x]$;
(*iii*) determinare $X = \{g \in \mathbb{Z}_{\bar{p}}[x] \mid (\forall a \in \mathbb{Z}_{\bar{p}})(f_{\bar{p}}(a) = \bar{0} \Rightarrow g(a) = \bar{0})\}$;
(*iv*) $h := \bar{2}x^3 + \bar{3}x + \bar{2}$ è associato a $f_{\bar{p}}$ in $\mathbb{Z}_{\bar{p}}[x]$?
(*v*) $t := \bar{3}x^3 - x + \bar{3}$ è associato a $f_{\bar{p}}$ in $\mathbb{Z}_{\bar{p}}[x]$?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
12 SETTEMBRE 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* Non è necessario consegnare la traccia.

Esercizio 1. Sia $(S, \leq)$ un insieme ordinato. Dire quando, per *definizione*, $(S, \leq)$ è un *reticolo*. Di ciascuna delle seguenti affermazioni dire se è vera o falsa:

(*i*) Ogni reticolo (non vuoto) ha massimo.
(*ii*) Per ogni reticolo L, ogni parte non vuota di L ha estremo superiore in L.
(*iii*) In ogni reticolo, gli elementi sono a due a due confrontabili.

Esercizio 2. Per ogni intero positivo n, rappresentato n in forma decimale (scritto quindi n come stringa di cifre '$c_t c_{t-1} \dots c_1 c_0$', dove $t \in \mathbb{N}$, ciascuno dei c_i è un intero compreso tra 0 e 9, $c_t \neq 0$ e $n = \sum_{i=0}^{t} 10^i c_i$), si ponga $s_n = \sum_{i=0}^{t} c_i$ (la somma delle cifre di n) e $p_n = \prod_{i=0}^{t} c_i$ (il prodotto delle cifre di n). Si consideri l'applicazione

$$f \colon n \in \mathbb{N}^* \longmapsto (s_n, p_n) \in \mathbb{N}^* \times \mathbb{N}$$

ed il suo nucleo di equivalenza σ.

(*i*) Si calcolino l'immagine $\vec{f}(\{10, 11\})$ e l'antiimmagine $\overleftarrow{f}(\{(1, 0)\})$.
(*ii*) f è iniettiva? f è suriettiva?
(*iii*) L'insieme quoziente $\mathbb{N}^*/\sigma$ è finito o infinito? $[40]_\sigma$ è finita o infinita?
(*iv*) Sia $S = \{1, 6, 15, 8, 30, 102, 51, 2001, 2411\}$. Descrivere in modo esplicito S/σ ed i suoi elementi, elencando gli elementi di ogni classe di equivalenza e specificando $|S/\sigma|$.

Sia ora ρ la relazione d'ordine definita da:

$$(\forall a, b \in \mathbb{N}^*)\big(a \ \rho \ b \iff (a = b) \vee (s_a < s_b \wedge p_a < p_b)\big)$$

(*v*) Determinare gli eventuali elementi minimali, massimali, minimo, massimo in $(\mathbb{N}^*, \rho)$. Stabilire se $(\mathbb{N}^*, \rho)$ è un reticolo.
(*vi*) Determinare in $(\mathbb{N}^*, \rho)$, se esiste, $\sup\{6, 15\}$.
(*vii*) Posto $X = \{3, 14, 20, 111, 121, 1111\}$, disegnare il diagramma di Hasse di (X, ρ) e stabilire se (X, ρ) è un reticolo. Nel caso lo sia, è distributivo?, è complementato?

Esercizio 3. Sia $S = \mathbb{Z}_{40} \times \mathbb{Z} \times \{1, -1\}$, e sia $*$ l'operazione binaria in S definita da:

$$\big(\forall (a, b, c), (u, v, w) \in S\big)\big((a, b, c) * (u, v, w) = (au, b + cv, cw)\big).$$

(*i*) $*$ è associativa? È commutativa? Ha elementi neutro a destra, a sinistra, elemento neutro in S? Che tipo di struttura algebrica è $(S, *)$?
(*ii*) Se la domanda ha senso, $(\overline{17}, 17, -1)$ è invertibile in $(S, *)$? E, nel caso, qual è il suo inverso?
(*iii*) Sempre se la domanda ha senso, determinare gli elementi invertibili in $(S, *)$ e descrivere l'inverso di un generico elemento invertibile (a, b, c) di S.
(*iv*) Si dica se $A := \mathbb{Z}_{40} \times \mathbb{N} \times \{1, -1\}$ è o non è una parte chiusa in $(S, *)$ e, se lo è, che tipo di struttura algebrica è $(A, *)$.

Esercizio 4. Sia $A = \{f \in \mathbb{Z}_7[x] \mid (\forall a \in \mathbb{Z}_7)(f(a) = \bar{0} \iff (a = \bar{2} \vee a = \bar{3}))\}$, l'insieme dei polinomi in $\mathbb{Z}_7[x]$ che abbiano come radici in $\mathbb{Z}_7$ le classi $\bar{2}$ e $\bar{3}$, e nessun'altra.

(*i*) Quali e quanti sono i polinomi di secondo grado in A? Quanti tra questi sono monici?
(*ii*) Quali e quanti sono i polinomi di terzo grado in A? Quanti tra questi sono monici?
(*iii*) Stabilire se il polinomio $g := (x^2 + \bar{2}x - \bar{1})(x^4 - \bar{2}x) \in \mathbb{Z}_7[x]$ appartiene ad A e, poi, scrivere g come prodotto di polinomi monici irriducibili in $\mathbb{Z}_7[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
12 OTTOBRE 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. (*i*) Dare la definizione di *partizione* di un insieme.

(*ii*) Sia $A = \{1, 2, 3, 4, 5, 6\}$. Fornire, se possibile, un esempio di partizione $\mathcal{F}$ di A tale che, detta σ la relazione di equivalenza associata a $\mathcal{F}$, valgano per σ queste tre proprietà:

$$1 \notin [3]_\sigma; \qquad \{1, 2\} \subseteq [4]_\sigma; \qquad [5]_\sigma \cap [6]_\sigma \neq \varnothing.$$

(*iii*) Quante sono, in tutto, le partizioni di A per le quali valga la condizione richiesta in (ii)?

Esercizio 2. Sia α la relazione binaria definita in $\mathbb{Q}$ da: $(\forall a, b \in \mathbb{Q})\big(a \ \alpha \ b \iff (\exists n \in \mathbb{Z})(b = a^n)\big)$.

(*i*) α è una relazione d'ordine? [Suggerimento: ogni numero razionale $a \neq 0$ ha inverso a^{-1}.] Se lo è, identificare gli eventuali minimo e massimo di $(\mathbb{Q}, \alpha)$.

Sia poi β la relazione binaria indotta da α su $\mathbb{Z}$, cioè quella definita da:

$$(\forall a, b \in \mathbb{Z})\big(a \ \beta \ b \iff (\exists n \in \mathbb{Z})(b = a^n)\big).$$

(*ii*) β è una relazione d'ordine? *[Suggerimento: nel ragionare sull'antisimmetria può essere utile considerare gli interi* 0, 1 *e* -1 *separatamente da tutti gli altri. Ricordare:* $0^0 = 1$.*]* Se lo è, identificare gli eventuali minimo e massimo di $(\mathbb{Z}, \beta)$ e rispondere anche alle domande che seguono.

(*iii*) Quali tra 0, 1, 2, 3 e 4 sono elementi minimali in $(\mathbb{Z}, \beta)$?

(*iv*) $(\mathbb{Z}, \beta)$ è un reticolo?

(*v*) Vero o falso?

(a) $(\forall n, m \in \mathbb{N})(2^n \ \beta \ 2^m \iff n \leq m)$;

(b) $(\forall n, m \in \mathbb{N})(2^n \ \beta \ 2^m \iff n \mid m)$.

(*vi*) Sia $X = \{2^n \mid n \in \mathbb{N}\}$. (X, β) è un reticolo?

(*vii*) Disegnare diagramma di Hasse di (Y, β), dove $Y = \{y \in X \mid y \leq 1000\}$.

Esercizio 3. Per ogni $m \in \mathbb{N}^*$, sia f_m l'applicazione: $x \in \mathbb{Z}_m \mapsto \overline{20}x + \overline{8} \in \mathbb{Z}_m$.

(*i*) Dimostrare che f_{49} è un'applicazione biettiva e scriverne l'inversa.

(*ii*) Caratterizzare gli elementi dell'insieme $M = \{m \in \mathbb{N}^* \mid f_m \text{ è biettiva}\}$ ed elencare gli elementi di $S := \{m \in M \mid m \leq 15\}$.

Esercizio 4. Sia $G = \mathcal{U}(\mathbb{Z}_9)$, il gruppo degli invertibili dell'anello $\mathbb{Z}_9$.

(*i*) Elencare gli elementi di G. Quanti sono?

Detto $E = \{1, -1\}$ il gruppo degli invertibili di $\mathbb{Z}$, sia $*$ l'operazione binaria in $G \times E$ definita ponendo, per ogni $a, b \in G$ e $\varepsilon, \delta \in E$, $\quad (a, \varepsilon) * (b, \delta) = (ab^\varepsilon, \varepsilon\delta)$.

(*ii*) Provare che $(G \times E, *)$ è un gruppo. È abeliano? Quanti elementi ha?

(*iii*) Provare che $\{(\bar{1}, 1), (\bar{8}, 1)\}$ è una parte chiusa di $G \times E$.

Esercizio 5. Vero o falso?

(*i*) Esiste un campo F tale che il polinomio $x^2 - 1$ sia irriducibile in $F[x]$.

(*ii*) Per ogni campo F, il polinomio $x^2 + 1$ è irriducibile in $F[x]$.

(*iii*) Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ammette radice in $\mathbb{R}$.

(*iv*) Ogni polinomio di grado dispari in $\mathbb{R}[x]$ non è irriducibile in $\mathbb{R}$.

(*v*) Per ogni intero $n \geq 6$, esiste in $\mathbb{Q}[x]$ un polinomio di grado n che non ammette radici in $\mathbb{Q}$ ed è prodotto di tre polinomi irriducibili.

Scrivere come prodotto di polinomi irriducibili in $F[x]$ il polinomo $x^4 - 2$ in ciascuno dei casi $F = \mathbb{R}$, $F = \mathbb{Q}$, $F = \mathbb{Z}_7$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
15 NOVEMBRE 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dare la definizione di *grafo* (semplice) e di *albero*.

Esercizio 2. Sia $S := \{n \in \mathbb{N} \mid (\forall X \subseteq \mathbb{N})(\{n\} \subseteq X)\}$. Descriverne gli elementi e calcolare $|S|$.

Esercizio 3. Sia A l'insieme delle applicazioni da $\mathbb{Z}_5$ a $\mathbb{Z}_5$.

(*i*) Calcolare $|A|$.

Si definiscano due operazioni, $+$ e $\cdot$, in A ponendo, per ogni $f, g \in A$,

$$f + g \colon x \in \mathbb{Z}_5 \mapsto f(x) + g(x) \in \mathbb{Z}_5; \qquad f \cdot g \colon x \in \mathbb{Z}_5 \mapsto f(x)g(x) \in \mathbb{Z}_5.$$

(*ii*) Date $f, g \in A$, definite ponendo $f(\bar{0}) = \bar{1}$ e $f(x) = \bar{2}$ per ogni $x \in \mathbb{Z}_5 \smallsetminus \{\bar{0}\}$; $g(\bar{1}) = g(\bar{2}) = \bar{4}$ e $g(x) = \bar{2}$ per ogni $x \in \mathbb{Z}_5 \smallsetminus \{\bar{1}, \bar{2}\}$, calcolare $f + g$ ed $f \cdot g$, precisando le immagini di ogni elemento di $\mathbb{Z}_5$.

(*iii*) A risulta essere un anello. È commutativo? È unitario? Qual è l'elemento neutro in $(A, +)$?

(*iv*) Per ogni $f \in A$, determinare l'opposto di f in A.

(*v*) Caratterizzare gli elementi invertibili in A (attraverso una proprietà delle immagini). Calcolare $|\mathcal{U}(A)|$.

(*vi*) Se possibile, determinare in A l'inverso del suo elemento f, definito da $f(\bar{2}) = \bar{3}$ e $f(x) = \bar{2}$ se $x \in \mathbb{Z}_5 \smallsetminus \{\bar{2}\}$.

(*vii*) L'insieme delle applicazioni iniettive appartenenti ad A è una parte chiusa in $(A, +)$?

Esercizio 4. Per ogni primo p si consideri, nell'anello di polinomi $\mathbb{Z}_p[x]$, la relazione di equivalenza σ_p definita ponendo, per ogni $f, g \in \mathbb{Z}_p[x]$, $f \ \sigma_p \ g$ se e solo se f e g hanno lo stesso grado.

(*i*) Calcolare la cardinalità delle classi $[x^2]_{\sigma_7}$ e $[x^2 + \bar{3}x - \bar{1}]_{\sigma_7}$ (in $\mathbb{Z}_7[x]$).

(*ii*) In generale, per ogni primo p ed ogni polinomio $f \in \mathbb{Z}_p[x]$, calcolare $|[f]_{\sigma_p}|$.

(*iii*) Vero o falso? Per ogni primo p ed ogni $f, g \in \mathbb{Z}_p[x]$,

(a) se $f \ \sigma_p \ g$, allora f e g sono associati;

(b) se f e g sono associati, allora $f \ \sigma_p \ g$;

(c) se $f \ \sigma_p \ g$ e $f = p_1 p_2 \cdots p_r$, $g = q_1 q_2 \cdots q_s$, dove $r, s \in \mathbb{N}^*$ e ciascuno dei polinomi p_i, q_j è irriducibile, allora esistono $i \in \{1, 2, \ldots, r\}$ e $j \in \{1, 2, \ldots, s\}$ tali che $p_i \ \sigma_p \ q_j$,

(d) scelti comunque $f_1, g_1 \in \mathbb{Z}_p[x]$, se $f \ \sigma_p \ f_1$ e $g \ \sigma_p \ g_1$, allora:

1.) $(f + g) \ \sigma_p \ (f_1 + g_1)$;

2.) $(fg) \ \sigma_p \ (f_1 g_1)$.

(*iv*) Per quali primi p (se ne esistono) i polinomi $f = \overline{60}x^4 + \overline{22}x^2 + \overline{8}x + \overline{7}$ e $g = \overline{210}x^3 + \overline{33}x^2 + \overline{10}x + \overline{5}$ di $\mathbb{Z}_p[x]$ verificano $f \ \sigma_p \ g$?

Esercizio 5. Si considerino le tre relazioni binarie α, β, γ in $\mathbb{N}$ definite da: per ogni $n, m \in \mathbb{N}$,

$$n \ \alpha \ m \iff \text{ogni divisore primo di } n \text{ divide } m;$$

$$n \ \beta \ m \iff (n \ \alpha \ m \wedge n < m); \qquad n \ \gamma \ m \iff (n \ \alpha \ m \wedge n \geq m)$$

Esattamente una tra queste è una relazione d'ordine (largo). Quale? (Spiegare in modo esauriente perché, e perché le altre non lo sono.) Rispetto ad essa,

(*i*) è vero che, per ogni $n \in \mathbb{N}$, n^2 è in relazione con n?

(*ii*) Si determinino gli eventuali elementi minimali, massimali, minimo, massimo e, se esiste, $\sup\{8, 27\}$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
13 DICEMBRE 2016

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dire per quali coppie $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ esistono quoziente e resto e come questi sono definiti (enunciare il relativo teorema).

Dato un campo F, dire per quali coppie $(f, g) \in F[x] \times F[x]$ esistono quoziente e resto e come questi sono definiti (enunciare il relativo teorema).

Determinare quoziente e resto nella divisione (in $\mathbb{Z}$) di a per b in ciascuno dei seguenti casi:

(i) $a = 15, \quad b = 4$ (ii) $a = 15, \quad b = -4$

(iii) $a = -15, \quad b = 4$ (iv) $a = -15, \quad b = -4$

Esercizio 2. Si consideri l'applicazione $\lambda\colon (f, g) \in \mathbb{Z}_7[x] \times \mathbb{Z}_7[x] \mapsto fg \in \mathbb{Z}_7[x]$ (cioè l'ordinaria moltiplicazione in $\mathbb{Z}_7[x]$).

(*i*) λ è iniettiva? λ è suriettiva?

(*ii*) Determinare i polinomi $h \in \mathbb{Z}_7[x]$ tali che $\lambda(\bar{5}, h) = x - \bar{1}$ (a questo scopo risolvere, esplicitando tutti i passaggi, un'opportuna equazione congruenziale).

(*iii*) Calcolare le antimmagini richieste, specificando per ciascuna se è finita o infinita e, se finita, quanti elementi ha:

(a) $A := \overleftarrow{\lambda}(\{\bar{0}\})$;

(b) $B := \overleftarrow{\lambda}(\{x - \bar{1}\})$;

(c) $C_p := \overleftarrow{\lambda}(\{p\})$ per un generico polinomio p irriducibile in $\mathbb{Z}_7[x]$.

(*iv*) Detto σ il nucleo di equivalenza di λ, descrivere $[(\bar{1}, x - \bar{1})]_\sigma$.

(*v*) Posto $K = \{s \in \mathbb{Z}_7[x] \mid s(\bar{1}) = \bar{0}\}$, determinare $\overleftarrow{\lambda}(K)$.

Esercizio 3. Nel monoide $(\mathbb{N}^{\mathbb{N}}, \circ)$ delle applicazioni di $\mathbb{N}$ in $\mathbb{N}$ (dove $\circ$ è l'ordinaria operazione di composizione tra applicazioni) si consideri la parte

$$F = \{f \in \mathbb{N}^{\mathbb{N}} \mid f \text{ è biettiva e } f(1) = 1\}.$$

(*i*) Verificare che F è una parte chiusa di $(\mathbb{N}^{\mathbb{N}}, \circ)$.

(*ii*) Rispetto all'operazione indotta, F è un gruppo?

(*iii*) Dare un esempio di applicazione non identica $g \in F$ e costruirne l'inverso g^{-1} in $(F, \circ)$.

(*iv*) Quante e quali sono le applicazioni $h \in F$ tali che: $(\forall x \in \mathbb{N} \smallsetminus \{2, 5\})(h(x) = x)$?

Esercizio 4. Per ogni $n \in \mathbb{N}^* \smallsetminus \{1\}$, scritto n nella forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, dove $t \in \mathbb{N}^*$, $p_1, p_2, \ldots, p_t$ sono primi positivi a due a due distinti tra loro e $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{N}^*$, poniamo:

$$s(n) = p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_t^{\alpha_t}$$

e definiamo la relazione d'ordine ρ in $\mathbb{N}^* \smallsetminus \{1\}$ ponendo, per ogni $a, b \in \mathbb{N}^* \smallsetminus \{1\}$,

$$a \; \rho \; b \iff \big(a = b \vee s(a) < s(b)\big).$$

(*i*) $(\mathbb{N}^* \smallsetminus \{1\}, \rho)$ è totalmente ordinato?

(*ii*) Si determinino in $(\mathbb{N}^* \smallsetminus \{1\}, \rho)$ gli eventuali elementi minimali, massimali, minimo, massimo.

(*iii*) Si descrivano in $(\mathbb{N}^* \smallsetminus \{1\}, \rho)$ gli insiemi dei maggioranti e dei minoranti di $X := \{13, 36\}$, e si determinino, se esistono, $\inf X$ e $\sup X$.

(*iv*) $(\mathbb{N}^* \smallsetminus \{1\}, \rho)$ è un reticolo?

(*v*) Sia $S = \{2, 3, 9, 13, 14, 21, 27, 36\}$. Disegnare il diagramma di Hasse di (S, ρ), decidere se (S, ρ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.

Corso di Laurea in Informatica — Corso di Algebra (I gruppo)
Esercizi — Grafi

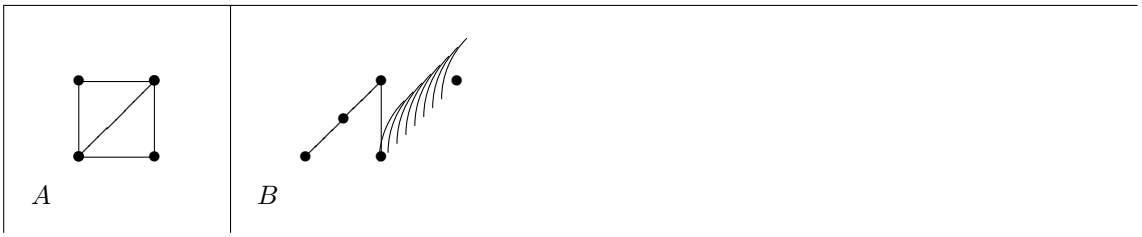
1. Un grafo G ha 7 lati e 8 vertici, sette dei quali hanno grado 1. Qual è il grado dell'ottavo vertice? Disegnare un grafo con queste proprietà. Esistono due siffatti grafi tra loro non isomorfi? Un tale grafo è un albero? Esistono grafi con 7 lati e 8 vertici che non siano alberi?

2. Esiste un grafo con 5 lati e almeno tre vertici di grado 4?

3. Un grafo connesso G ha 9 vertici. Di questi, almeno 6 sono pari. Questi dati sono sufficienti per stabilire se G ha cammini euleriani?

4. Sia G un grafo planare (cioè piano) connesso con 7 vertici e 8 lati. Quante facce ha G se disegnato sul piano in modo che i lati si intersechino solo in vertici?

5. Cercare tutte le coppie di grafi tra loro isomorfi fra quelli qui disegnati. Di ciascuno dei grafi di dica poi se è connesso (individuando nel caso contrario le componenti connesse), se è un albero e se è una foresta, si indichi il grado di ciascun vertice e si stabilisca se il grafo ha o meno un circuito o un cammino euleriano (nel caso ve ne siano, descriverne qualcuno). Si decida poi se il grafo è planare. Infine, ove possibile, se ne determini un sottoalbero massimale (ovvero albero di supporto, cioè un sottografo che sia un albero e che abbia gli stessi vertici del grafo dato).



Corso di Laurea in Informatica — Corso di Algebra (I gruppo)
Esercizi — Tautologie, Insiemi, Aritmetica

1. Quali delle seguenti sono tautologie?

a. $(a \vee \neg b) \iff (a \Rightarrow b)$

b. $(a \vee \neg b) \iff (b \Rightarrow a)$

c. $\big((a \Rightarrow b) \wedge (\neg a \Rightarrow b)\big) \Longrightarrow \big(c \Longrightarrow b\big)$

2. Stabilire quali tra le seguenti sono vere per ogni possibile scelta degli insiemi A, B, C. Utilizzare, se lo si ritiene opportuno, diagrammi di Euler-Venn.

a. $A - (B \cup C) = (A - B) \cup (A - C)$

b. $(B \cup C) - A = (B - A) \cup (C - A)$

c. $A \cup B = A \iff A \cap B = B$

d. $(A \cup B) \cap C = A \cup (B \cap C)$

3. Dire quali delle seguenti sono corrette definizioni di applicazioni. Tra le applicazioni quali sono iniettive, suriettive, biettive?

a. $n \in \mathbb{N} \longmapsto n - 1 \in \mathbb{N}$

b. $n \in \mathbb{Z} \longmapsto n - 1 \in \mathbb{Z}$

c. $n \in \mathbb{Z} \longmapsto 7n - n^2 \in \mathbb{Z}$

d. $n \in \mathbb{N} \longmapsto \begin{cases} 3^n \cdot 5^{n+1}, & \text{se } n \notin 2\mathbb{N} \\ 7n/2, & \text{se } n \in 2\mathbb{N} \end{cases} \in \mathbb{N}$

e. $(X, Y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \longmapsto (X \cup \{13, 14\}) - Y \in \mathcal{P}(\mathbb{N})$

f. $n \in \mathbb{Z} \longmapsto \begin{cases} 2n, & \text{se } 3|n \\ n - 4, & \text{se } n \equiv 1 \pmod 3 \\ 2n + 5, & \text{se } n \equiv -1 \pmod 3 \end{cases} \in 3\mathbb{Z}$

4. Siano $f : n \in \mathbb{Z} \mapsto |n| + 1 \in \mathbb{N}^{\#}$ e $g : m \in \mathbb{N}^{\#} \mapsto (m-1)^2 + 2 \in \mathbb{N}$. Scrivere l'applicazione composta fg

ESERCIZI

1. Scrivere le tavole di verità di queste forme proposizionali e decidere quali tra esse sono tautologie:

$p \vee (p \Rightarrow q)$; $\quad (p \vee q) \Rightarrow p$; $\quad (p \text{ XOR } q) \Rightarrow p$; $\quad (p \wedge q) \Rightarrow p$; $\quad (p \vee q) \Rightarrow r$; $\quad (p \wedge q) \Rightarrow r$.

2. Di ciascuna di queste forme proposizionali si decida se è una tautologia, se è contingente, se è una contraddizione; non è necessario scriverne la tavola di verità:

$$p \iff (p \iff p); \qquad (p \text{ XOR } q) \iff ((\neg q) \iff p); \qquad ((\neg p) \Rightarrow q) \iff ((\neg q) \Rightarrow p);$$
$$\big((p_1 \Rightarrow q) \vee (p_2 \Rightarrow q) \vee (p_3 \Rightarrow q) \vee (p_4 \Rightarrow q) \vee (p_5 \Rightarrow q)\big) \Longrightarrow \big((p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5) \Rightarrow q\big);$$
$$\big((p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5) \Rightarrow q\big) \Longrightarrow \big((p_1 \Rightarrow q) \vee (p_2 \Rightarrow q) \vee (p_3 \Rightarrow q) \vee (p_4 \Rightarrow q) \vee (p_5 \Rightarrow q)\big);$$
$$\big((p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q) \wedge (p_4 \Rightarrow q) \wedge (p_5 \Rightarrow q)\big) \iff \big((p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5) \Rightarrow q\big);$$

3. Negare le frasi (o le formule, dove $\varphi, \psi, \theta, \eta$ indicano predicati):

(*i*) Se Aldo incontra Bice, Carlo va in bicicletta e Dario lo insegue;
(*ii*) Ogni mese dell'anno prossimo ci sarà un giorno in cui pioverà;
(*iii*) Esiste, in Italia, una città in cui se il sindaco è alto più di due metri allora ogni abitante è biondo;
(*iv*) $\big((\forall x)(\varphi(x))\big) \Longrightarrow \big((\exists y)(\psi(y))\big)$;
(*v*) $(\forall x)\big(\exists y\big((\varphi(x) \wedge \psi(y)) \Rightarrow (\theta(x,y) \vee \eta(y))\big)\big)$.

4. Rappresentare con diagrammi di Euler-Venn le espressioni insiemistiche $(A \cup B) \smallsetminus C$, $\quad (A \smallsetminus B) \triangle (B \smallsetminus C)$, $(A \triangle C) \triangle B$ $\quad$ e $\quad (A \smallsetminus C) \triangle B$. Decidere poi quali tra queste formule sono vere e quali false, fornendo per quelle false un controesempio esplicito:

(*i*) $(\forall A, B, C)\big((A \cup B) \smallsetminus C \subseteq (A \smallsetminus B) \triangle (B \smallsetminus C)\big)$;
(*ii*) $(\forall A, B, C)\big((A \smallsetminus B) \triangle (B \smallsetminus C) \subseteq (A \cup B) \smallsetminus C\big)$;
(*iii*) $(\forall A, B, C)\big((A \triangle C) \triangle B \subseteq (A \smallsetminus C) \triangle B\big)$;
(*iv*) $(\forall A, B, C)\big((A \smallsetminus C) \triangle B \subseteq (A \triangle C) \triangle B\big)$.

Vero o falso: $(\exists A, B, C)\big((A \smallsetminus C) \triangle B = C\big)$?

5. Vero o falso?

(*i*) $13 \in \{x \in \mathbb{Z} \mid x > 0 \text{ XOR } x < 0\}$;
(*ii*) $-5 \in \{x \in \mathbb{Z} \mid x > 0 \Rightarrow x = 7\}$;
(*iii*) $\{x \mid x = x \Rightarrow x \neq x\} = \{x \mid x = x \wedge x \neq x\}$;
(*iv*) $(\exists x)(x \in \varnothing)$;
(*v*) $(\exists x)(x \in \{\varnothing\})$;
(*vi*) $(\exists x \in \mathcal{P}(\mathbb{Z}))(x \in \{\varnothing\})$;
(*vii*) $(\exists x \in \mathcal{P}(\mathbb{Z}))(x \notin \{\varnothing\})$;
(*viii*) $(\forall x, y)\big(\{x, y\} = \{y, x\}\big)$;
(*ix*) $(\forall x, y)\big((x, y) = (y, x)\big)$;
(*x*) $(\exists x, y)\big((x, y) = (y, x)\big)$;

6. Siano, per ogni $i \in \mathbb{Z}$, $X_i = \{n \in \mathbb{Z} \mid n \leq i\}$ e $Y_i = \{n \in \mathbb{Z} \mid i \leq n\}$; sia poi $A = \{n^2 \mid n \in \mathbb{Z}\}$. Calcolare:

$$X_0; \qquad X_3 \cap Y_7; \qquad X_3 \cup Y_{-1}; \qquad X_0 \triangle Y_1; \qquad A \cap Y_{12}; \qquad \bigcap_{i \in \mathbb{N}} X_i; \qquad \bigcup_{i \in \mathbb{N}} X_i.$$

7. Quali tra queste sono bene definite come applicazioni e quali sono applicazioni suriettive?

(*i*) $n \in \mathbb{N} \mapsto -3n/2 \in \mathbb{Z}$

(*ii*) $n \in \mathbb{Z} \mapsto \begin{cases} n+1 & \text{se } n \text{ è pari} \\ n-1 & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{Z}$

(*iii*) $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cup \mathbb{N} \in \mathcal{P}(\mathbb{Z})$

(*iv*) $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cap \mathbb{N} \in \mathcal{P}(\mathbb{Z})$

(*v*) $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \cap \mathbb{N} \in \mathcal{P}(\mathbb{N})$

(*vi*) $X \in \mathcal{P}(\mathbb{Z}) \mapsto X \triangle \mathbb{N} \in \mathcal{P}(\mathbb{Z})$

(*vii*) $X \in \mathcal{P}(\mathbb{Z}) \mapsto \mathbb{Z} \smallsetminus X \in \mathcal{P}(\mathbb{Z})$.

Avendo posto $\mathcal{C}(\mathbb{Z}) = \{\{a, b\} \mid a, b \in \mathcal{P}(\mathbb{Z})\}$:

(*viii*) $\{a, b\} \in \mathcal{C}(\mathbb{Z}) \mapsto a \cap (b \cap \mathbb{N}) \in \mathcal{P}(\mathbb{Z})$

(*ix*) $\{a, b\} \in \mathcal{C}(\mathbb{Z}) \mapsto a \cap (b \cap \mathbb{N}) \in \mathcal{P}(\mathbb{N})$

(*x*) $\{a, b\} \in \mathcal{C}(\mathbb{Z}) \mapsto a \cap (b \cup \mathbb{N}) \in \mathcal{P}(\mathbb{Z})$.

Avendo posto $M = \mathrm{Map}(\mathbb{N}, \mathbb{Z})$, l'insieme delle applicazioni da $\mathbb{N}$ a $\mathbb{Z}$:

(*xi*) $f \in M \longmapsto f(3) \in \mathbb{N}$

(*xii*) $f \in M \longmapsto (f(3))^2 \in \mathbb{N}$

(*xiii*) $f \in M \longmapsto f(3) \in \mathbb{Z}$

(*xiv*) $f \in M \longmapsto f(3) + 1 \in \mathbb{Z}$.

8. Descrivere in modo esplicito $h = g \circ f$ e stabilire quali tra f, g e h sono suriettive nei seguenti casi:

(*i*) Posto $S = \{1, 2\}$ e $T = S \cup \{3\}$, $f\colon S \to S$ e $g\colon S \to T$ definite da: $f(1) = 2 = g(1)$ e $f(2) = 1 = g(2)$ (domanda supplementare: si ha $f = g$?);

(*ii*) $f\colon n \in \mathbb{Z} \mapsto \{n\} \in \mathcal{P}(\mathbb{Z})$ e $g\colon X \in \mathcal{P}(\mathbb{Z}) \mapsto \mathbb{N} \smallsetminus X \in \mathcal{P}(\mathbb{N})$;

(*iii*) $f\colon n \in \mathbb{Z} \mapsto n^2 + 1 \in \mathbb{Z}$ e $g = f$;

(*iv*) $f\colon n \in \mathbb{Z} \mapsto n^2 + 3 \in \mathbb{N}$ e $g\colon n \in \mathbb{N} \mapsto \begin{cases} 3n & \text{se } n > 2 \\ n^3 & \text{se } n \leq 2 \end{cases} \in \mathbb{Z}$.

9. Si studino le operazioni binarie qui definite, cercando di stabilire se sono commutative, associative, se ammettono elementi neutri a destra, elementi neutri a sinistra, elementi neutri, quali elementi della struttura algebrica che definiscono sono simmetrizzabili a destra, simmetrizzabili a sinistra, simmetrizzabili; che tipo di struttura algebrica è quella ottenuta:

(*i*) l'operazione potenza: $(a, b) \in \mathbb{N} \times \mathbb{N} \mapsto a^b \in \mathbb{N}$, [1]

(*ii*) le operazioni $*$, $\odot$ e $\bullet$ definite in $\mathbb{Z}$ da:

$$(\forall a, b \in \mathbb{Z}) \quad \big(\quad a * b = 2a + b \quad \wedge \quad a \odot b = 2 + a + b \quad \wedge \quad a \bullet b = ab + 2(a + b + 1) \quad \big);$$

(*iii*) in $\mathcal{P}(\mathbb{Z})$, l'operazione $*$ definita da: $(\forall A, B \in \mathcal{P}(\mathbb{Z}))(A * B = (A \smallsetminus \{1\}) \cap B)$;

(*iv*) in $\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$, le operazioni $*$, $\odot$ e $\bullet$ definite da: $\forall a, b, x, y \in \mathcal{P}(\mathbb{N})$

$$(a, b) * (x, y) = (a \cup y, b \cap y)$$
$$(a, b) \odot (x, y) = (a \cup x, b \cap y)$$
$$(a, b) \bullet (x, y) = (a \cup y, b \cap x)$$

Per ciascuna delle operazioni definite in (*ii*), si stabilisca quali tra $\mathbb{N}$, $2\mathbb{Z}$ (l'insieme dei numeri interi pari), $\mathbb{Z} \smallsetminus 2\mathbb{Z}$ (l'insieme dei numeri interi dispari) sono, rispetto all'operazione data, parti chiuse. $\mathcal{P}(\mathbb{N})$ è chiusa rispetto all'operazione definita in (*iii*)? Rispetto a quali delle operazioni definite in (*iv*) è chiusa $\mathcal{P}(\mathbb{N}) \times \{\{3\}\}$?

[1] a scanso di equivoci: 0^0 è definito come 1.

Corso di Laurea in Informatica — Corso di Algebra (I gruppo)
Esercizi — Polinomi e Strutture Algebriche

1. Determinare il massimo comun divisore monico in $\mathbb{Q}[x]$ per ciascuna della seguenti coppie di polinomi:
a. $x^{10}+1$ e x^7+1;
b. $x^{10}-1$ e x^7-1;
c. x^4-x-2 e $3x^3+6x^2-3$;
d. $2x^4+3x^3-2x-3$ e $2x^6+3x^5+2x^3+3x^2-2x-3$;

2. Determinare, se esistono, polinomi u e v in $\mathbb{Q}[x]$ tali che:
a. $(x^{10}+1)u+(x^7+1)v=1$;
b. $(x^{10}+1)u+(x^7+1)v=x$;
c. $(x^{10}-1)u+(x^7-1)v=1$;
d. $(x^{10}-1)u+(x^7-1)v=2x-2$;
e. $(x^5+2)u+(x^4-1)v=3$.

3. [*Da affrontare dopo aver completato lo studio dei polinomi*] Sia $f=x^3-x^2-2x+2\in\mathbb{Q}[x]$. Dopo aver verificato che 1 è radice di f, scrivere $f\ldots$
a. $\ldots$ come prodotto di polinomi monici irriducibili in $\mathbb{Q}[x]$;
b. $\ldots$ come prodotto di polinomi monici irriducibili in $\mathbb{R}[x]$.

4. Studiare le seguenti operazioni, stabilendo per ciascuna di esse se è un'operazione associativa, commutativa, se ammette elemento neutro.
a. $(n,m)\in\mathbb{Z}\times\mathbb{Z}\longmapsto n-m\in\mathbb{Z}$;
b. $(x,y)\in\mathbb{N}\times\mathbb{N}\longmapsto y\in\mathbb{N}$;
c. $(A,B)\in\mathcal{P}(\mathbb{N})\times\mathcal{P}(\mathbb{N})\longmapsto\mathbb{N}\smallsetminus(A\cup B)\in\mathcal{P}(\mathbb{N})$;
d. $(X,Y)\in\mathcal{P}(\mathbb{N})\times\mathcal{P}(\mathbb{N})\longmapsto X\cup\{1\}\cup Y\in\mathcal{P}(\mathbb{N})$.

5. Considerare le operazioni binarie $\oplus$ e $\odot$ definite in $\mathbb{Z}$ da: $\forall\, u,v\in\mathbb{Z}$

$$u\oplus v:=u+v+1;\qquad\qquad u\odot v:=uv+u+v.$$

Decidere se $\mathbb{Z}$ munito di queste due operazioni è un anello. Nel caso, stabilire se si tratta di un anello commutativo, di un anello unitario, di un anello booleano, di un campo e calcolarne la caratteristica.

6. Tra i seguenti anelli dire quali sono unitari, quali commutativi, quali integri, quali campi:

$$\mathbb{Z}_{13},\quad \mathbb{Z}_{14},\quad \mathbb{Z}_{15},\quad 3\mathbb{Z},\quad \mathbb{Z},\quad \mathbb{Z}[x],\quad \mathbb{Z}_3[x],\quad \mathbb{Z}_4[x],\quad \mathrm{M}_2(\mathbb{R}).$$

7. Per ciascuno dei seguenti anelli elencare gli elementi invertibili, i divisori dello zero, gli elementi nilpotenti, gli elementi idempotenti: $\mathbb{Z}_9$, $\mathbb{Z}_{18}$, $\mathbb{Z}_{17}$, $\mathbb{Z}_8$, $\mathbb{Z}$, $\mathrm{M}_2(\mathbb{Z}_2)$.

8. [*Da affrontare dopo aver completato lo studio dei polinomi*] Determinare tutte le radici in $\mathbb{Z}_{12}$ del polinomio $x^2-1\in\mathbb{Z}_{12}[x]$. Se il loro numero non sembra sorprendente o si è studiato troppo poco oppure piuttosto bene. Rifletterci sopra.

9. Date comunque quattro parti A, B, C, D di $\mathbb{R}$ si ponga

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}:=\left\{\left.\begin{pmatrix}a & b\\ c & d\end{pmatrix}\right|a\in A,\ b\in B,\ c\in C,\ d\in D\right\}.$$

Si ponga anche $\mathbf{0}:=\{0\}$ e $\mathbf{1}:=\{1\}$. Per ciascuna delle seguenti parti dell'anello $\mathrm{M}_2(\mathbb{R})$ delle matrici 2×2 su $\mathbb{R}$ stabilire se si tratta o meno di un sottoanello, di un sottoanello unitario, di un ideale destro, di un ideale sinistro di $\mathrm{M}_2(\mathbb{R})$, di un sottogruppo del gruppo additivo di $\mathrm{M}_2(\mathbb{R})$.

$$\begin{pmatrix}\mathbb{Q} & \mathbb{Q}\\ \mathbf{0} & \mathbb{Q}\end{pmatrix},\quad \begin{pmatrix}\mathbb{Z} & \mathbb{R}\\ \mathbf{0} & \mathbb{Z}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbb{Q} & \mathbf{0}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbb{R}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ \mathbb{R} & \mathbb{R}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbb{Q}\\ \mathbf{0} & \mathbb{R}\end{pmatrix},\quad \begin{pmatrix}\mathbf{1} & \mathbf{0}\\ \mathbf{0} & \mathbb{R}\end{pmatrix}.$$

Ripetere lo stesso esercizio per l'anello $\mathrm{M}_2(\mathbb{Z})$ e le sue parti

$$\begin{pmatrix}\mathbb{Z} & \mathbb{Z}\\ \mathbf{0} & \mathbb{Z}\end{pmatrix},\quad \begin{pmatrix}2\mathbb{Z} & \mathbb{Z}\\ \mathbf{0} & \mathbb{Z}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ 1+3\mathbb{Z} & \mathbf{0}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ 3\mathbb{Z} & 5\mathbb{Z}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbf{0}\\ 3\mathbb{Z} & 3\mathbb{Z}\end{pmatrix},\quad \begin{pmatrix}\mathbf{0} & \mathbb{N}\\ \mathbf{0} & \mathbb{N}\end{pmatrix}.$$

10. Con notazioni analoghe a quelle dell'esercizio precedente stabilre se, munito del prodotto righe per colonne, l'insieme $\left(\begin{smallmatrix}\mathbf{1} & \mathbb{Q}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$ costituisce un gruppo e quali tra $\left(\begin{smallmatrix}\mathbf{1} & \mathbb{Z}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{1} & 2\mathbb{Z}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{1} & \mathbf{1}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{1} & \mathbb{N}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{1} & \mathbb{N}^{\#}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{1} & 1+3\mathbb{Z}\\ \mathbf{0} & \mathbf{1}\end{smallmatrix}\right)$ ne sono sottogruppi. Quali tra i precedenti sono parti stabili (quindi semigruppi) e quali monoidi?

Corso di Laurea in Informatica — Corso di Algebra (I gruppo)
Esercizi — Relazioni binarie

1. Ciascuno dei seguenti insiemi è il grafico di una relazione binaria in $\mathbb{Z}$. Studiare le relazioni così definite, stabilendo per ciascuna di essa se si tratta di una relazione riflessiva, simmetrica, transitiva, antisimmetrica, antiriflessiva, di una relazione d'equivalenza, di un ordinamento.

a. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid n+m \text{ è pari}\}$;
b. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid n = m \text{ oppure } n+m \text{ è multiplo di } 3\}$;
c. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid n < 3m\}$;
d. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid n^2 < m^2\}$;
e. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid n^2 \leq m^2\}$;
f. $\{(n,m) \in \mathbb{N}\times\mathbb{N} \mid n \equiv m \pmod{12}\}$;
g. $\{(n,m) \in \mathbb{Z}\times\mathbb{Z} \mid 6 \text{ divide } 2n+3m\}$.

2. Ripetere lo stesso esercizio per le relazioni binarie definite come segue:

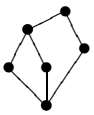
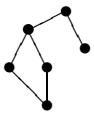
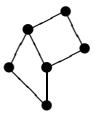
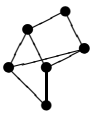
a. ρ', definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{Z})$, $X\ \rho'\ Y \iff (\exists \min X \wedge \exists \min Y \wedge \min X = \min Y)$;
b. ρ, definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{Z})$, $X\ \rho\ Y \iff \big((\exists \min X \wedge \exists \min Y) \Rightarrow \min X = \min Y\big)$;
c. τ, definita in $X = \{a,b,c,d\}$, dove $|X| = 4$, con grafico $\{(a,a),(b,c),(a,d),(c,b),(c,c),(b,b)\}$;
d. σ, definita in $\mathbb{N}$ ponendo, per ogni $x, y \in \mathbb{N}$, $x\ \sigma\ y \iff x \neq y$;
e. ψ, definita in $\mathcal{P}(\mathbb{N})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{N})$, $X\ \psi\ Y \iff |X \cap Y| = 3$.

3. Con riferimento all'esercizio precedente, decidere quali tra le seguenti valgono:

$$\mathbb{N}\ \rho\ \mathbb{N}^{\#}, \qquad \mathbb{N}\ \rho\ \big(\mathbb{N} - \{32,14,87\}\big), \qquad \mathbb{Z}\ \rho\ \mathbb{N}^{\#}, \qquad \mathbb{Z}\ \rho\ (\mathbb{Z} - \mathbb{N}), \qquad \mathbb{Z}\ \rho\ (\mathbb{Z} - \mathbb{N}^{\#}),$$
$$(\mathbb{Z} - \mathbb{N}^{\#})\ \rho\ \varnothing, \qquad \{1\}\ \rho\ \{2\}, \qquad \{1\}\ \rho\ \{1,2\}; \qquad d\ \tau\ a; \qquad 5\ \sigma\ 55;$$
$$\mathbb{N}\ \psi\ \mathbb{N}, \qquad \mathbb{N}\ \psi\ \mathbb{N}^{\#}, \qquad \mathbb{N}\ \psi\ \{1,2,3\}, \qquad \{n \in \mathbb{N} \mid n > 12\}\ \psi\ \{n \in \mathbb{N} \mid n \leq 20 \wedge\ n \text{ è primo}\}.$$

4. Sia ρ la relazione binaria in $\mathcal{P}(\mathbb{N})$ definita da: $\forall X, Y \in \mathcal{P}(\mathbb{N})\ \big(X\ \rho\ Y \iff |X| = |Y|\big)$. Verificare che ρ è una relazione di equivalenza e descrivere le classi di equivalenza modulo ρ di $\varnothing$, $\mathbb{N}$, $\{n \in \mathbb{N} \mid n > 12\}$. Descrivere l'insieme quoziente $\mathcal{P}(\mathbb{N})/\rho$, stabilendo, in particolare, se si tratta di un insieme finito o infinito e, nel primo caso, quanti elementi ha. Ripetere lo stesso esercizio dopo aver sostituito ρ con τ, definita da: $\forall X, Y \in \mathcal{P}(\mathbb{N})\ \big(X\ \tau\ Y \iff (2 \in X \cap Y \vee 2 \notin X \cup Y)\big)$.

5. Tra i seguenti, dire quali sono diagrammi di Hasse di un reticolo, di un reticolo distributivo, di un'algebra di Boole:

(a)  (b)  (c)  (d) 

6. Sia $X = \{a,b,c,d,e,f,g,h\}$, in modo che valga $|X| = 8$. Verificare che la relazione binaria ρ in X, di grafico

$$\{(a,b),(a,c),(a,d),(a,e),(a,f),(a,g),(a,h),(b,d),(b,e),(b,f),(b,g),(b,h),$$
$$(c,d),(c,e),(c,f),(c,g),(c,h),(d,e),(d,f),(d,g),(d,h),(e,f),(g,f)\}$$

è un ordinamento in X e disegnarne il diagramma di Hasse. Rispetto a questo ordinamento si indichino gli eventuali minimo, massimo, elementi minimali, elementi massimali di X. Se esistono, si calcolino $\sup\{b,c,h\}$, $\inf\{b,c,h\}$, $\sup\{b,e,h\}$, $\inf\{b,e,h\}$. Quali elementi di X sono confrontabili con ogni altro elemento di X? Infine si stabilisca se X, ordinato da ρ, è un insieme totalmente ordinato, un reticolo, un reticolo completo, un reticolo distributivo, un'algebra di Boole.

7. Si considerino le seguenti parti di $\mathcal{P}(\mathbb{Z})$. Per ciascuna si stabilisca se essa, munita della relazione di inclusione, costituisce un insieme ordinato, un insieme totalmente ordinato, un reticolo, un reticolo completo, un reticolo distributivo, un'algebra di Boole, una sottoalgebra dell'algebra di Boole $\mathcal{P}(\mathbb{Z})$. Se ne indichino inoltre, caso per caso, gli eventuali minimo, massimo, elementi minimali, elementi massimali.

a. $\mathcal{P}_{\mathrm{f}}(\mathbb{Z})$ (cioè l'insieme delle parti finite di $\mathbb{Z}$);
b. $\mathcal{P}(\mathbb{Z}) - \mathcal{P}_{\mathrm{f}}(\mathbb{Z})$ (cioè l'insieme delle parti infinite di $\mathbb{Z}$);
c. $\mathcal{P}_{\mathrm{f}}(\mathbb{Z}) \cup \{X \in \mathcal{P}(\mathbb{Z}) \mid \mathbb{Z} - X \text{ è finito}\}$.

Cambia qualcosa, in questo esercizio, se si sostituisce a $\mathbb{Z}$ un qualsiasi insieme infinito?

8. Sia D l'insieme dei divisori positivi di 42, e sia $X = \{1,2,3\}$. Verificare che D, ordinato rispetto alla divisibilità, costituisce un'algebra di Boole. Disegnarne il diagramma di Hasse. Scrivere un isomorfismo di algebre di Boole da D a $\mathcal{P}(X)$. Quali sono gli insiemi Y tali che, come algebre di Boole, D e $\mathcal{P}(Y)$ siano isomorfi? L'insieme dei divisori positivi di 44, ordinato rispetto alla divisibilità, costituisce un'algebra di Boole? Indicare un numero naturale n diverso da 42 tale che l'insieme dei divisori positivi di n, sempre ordinato rispetto alla divisibilità, costituisca un'algebra di Boole isomorfa a X. È possibile scegliere n in modo che sia compreso tra 10 e 20?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
17 GENNAIO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dare la definizione di polinomio *irriducibile* (a coefficienti in un campo).

Esercizio 2. Dati gli insiemi $S := \{1, 3, 8, 15, 22\}$ e $X := \{3, 5, 7\}$, si determinino, elencandone gli elementi:

$$A = \{p \in X \mid (\exists x \in S)(p|x)\}; \qquad B = \{p \in X \mid (\exists! x \in S)(p|x)\};$$
$$C = \{p \in X \mid (\exists! x \in S)(p \nmid x)\}; \qquad D = \{p \in X \mid (\forall x \in S)(p \nmid x)\}.$$

(*i*) L'insieme costituito da alcuni di questi quattro insiemi è una partizione di X. Determinarlo.
(*ii*) Detta F questa partizione, descrivere l'insieme delle coppie ordinate in $X \times X$ che costituisce la relazione di equivalenza corrispondente a F.

Esercizio 3. Si consideri l'applicazione $f\colon x \in \mathbb{N} \mapsto \mathrm{rest}(x, 8) \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

(*i*) f è iniettiva? f è suriettiva?
(*ii*) Detto σ il nucleo di equivalenza di f, quante sono le classi di equivalenza in $\mathbb{N}/\sigma$? Descrivere esplicitamente gli elementi di ciascuna classe.
(*iii*) Scrivere un'applicazione biettiva da $[0]_\sigma$ a $[1]_\sigma$.

Definiamo la relazione d'ordine Σ in $\mathbb{N}$ ponendo, per ogni $x, y \in \mathbb{N}$,

$$x \,\Sigma\, y \iff \big(x = y \vee f(x) \text{ divide propriamente } f(y)\big).$$

(*iv*) Si determinino in $(\mathbb{N}, \Sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo. $(\mathbb{N}, \Sigma)$ è un reticolo?
(*v*) Disegnare il diagramma di Hasse di (L, Σ), dove $L = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Stabilire se (L, Σ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.

Esercizio 4. Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}_{20}$ da:

$$(\forall a, b \in \mathbb{Z}_{20}) \qquad a * b = ab - a + \bar{3}b - \bar{6}.$$

(*i*) Per ogni a e b in $\mathbb{Z}_{20}$, calcolare $a * \bar{0}$ e $\bar{0} * b$.
(*ii*) Sfruttando quanto appena fatto,
  (a) calcolare $\bar{1} * \bar{0}$ e $\bar{0} * \bar{1}$; decidere se $*$ è commutativa;
  (b) calcolare $(\bar{0} * \bar{1}) * \bar{0}$ e $\bar{0} * (\bar{1} * \bar{0})$; decidere se $*$ è associativa;
  (c) determinare tutti i $b \in \mathbb{Z}_{20}$ tali che $\bar{0} * b = \bar{0}$. Usare questo risultato per stabilire se $(\mathbb{Z}_{20}, *)$ è dotata di elementi neutri a destra;
  (d) stabilire se $(\mathbb{Z}_{20}, *)$ è dotata di elementi neutri a sinistra.

Sia $Y = \{[n]_{20} \mid n \in \mathbb{Z} \wedge n \equiv_5 2\}$. È possibile dimostrare che, per ogni $a \in \mathbb{Z}_{20}$ e $b \in Y$,

$$a * b = ab - a - b + \bar{2}. \tag{$\mathcal{P}$}$$

Utilizzando questa proprietà ($\mathcal{P}$):

(*iii*) verificare che Y è una parte chiusa di $(\mathbb{Z}_{20}, *)$;
(*iv*) stabilire se l'operazione indotta da $*$ su Y è associativa e se è commutativa. $(Y, *)$ ha elemento neutro?
(*v*) Nel caso la domanda abbia senso, per ciascuno di $\overline{7}$ e $\overline{12}$ stabilire se è invertibile in $(Y, *)$ e, se lo è, trovarne l'inverso.
(*vi*) Dimostrare la proprietà ($\mathcal{P}$).

Esercizio 5. Per ogni primo (positivo) p si consideri il polinomio

$$f_p = x^4 + x^3 - \overline{35}x^2 - \overline{36}x + \overline{34} \in \mathbb{Z}_p[x].$$

Dopo aver enunciato il teorema di Ruffini generalizzato,

(*i*) lo si usi per determinare l'insieme T dei primi p tali che f_p sia divisibile (in $\mathbb{Z}_p[x]$) per $x^2 - \overline{1}$.
(*ii*) Per ogni $p \in T$ si scriva f_p come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
10 FEBBRAIO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Negare le frasi:

(*i*) Per ogni $x \in \mathbb{Z}$ esiste $y \in \mathbb{Z}$ tale che $xy = x$.
(*ii*) Per ogni $X \in \mathcal{P}(S)$ esiste $Y \in \mathcal{P}(S)$ tale che $X \cap Y \subset X$.

Esercizio 2. In $M_2(\mathbb{Z}_{16})$ si consideri il sottoinsieme $G = \left\{ \begin{pmatrix} a & b \\ \bar{0} & \bar{1} \end{pmatrix} \middle| a \in \mathcal{U}(\mathbb{Z}_{16}) \wedge b \in \mathbb{Z}_{16} \right\}$.

(*i*) Determinare $|G|$.
(*ii*) Verificare che G è chiuso rispetto alla moltiplicazione (righe per colonne) tra matrici, che $(G, \cdot)$ è un gruppo e che non è abeliano.
(*iii*) Determinare l'inverso di $\left(\begin{smallmatrix} \bar{7} & \bar{1} \\ \bar{0} & \bar{1} \end{smallmatrix}\right)$ in $(G, \cdot)$.

Sia $H := \left\{ \left(\begin{smallmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{smallmatrix}\right), B \right\}$, dove $B = \left(\begin{smallmatrix} \bar{1} & \bar{8} \\ \bar{0} & \bar{1} \end{smallmatrix}\right)$.

(*iv*) Verificare che B coincide col suo inverso in $(G, \cdot)$.
(*v*) Verificare prima che H è una parte chiusa in $(G, \cdot)$, poi che H è un sottogruppo di $(G, \cdot)$.

Sia $\mathcal{R}$ la relazione binaria definita in G ponendo, per ogni $x, y \in G$, $\quad x \mathcal{R} y \iff x^{-1}y \in H$.

(*vi*) Ricordando che per ogni $x, y \in G$ si ha $y^{-1}x = (x^{-1}y)^{-1}$, verificare che $\mathcal{R}$ è una relazione di equivalenza in G.
(*vii*) Calcolare $\left[\left(\begin{smallmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{smallmatrix}\right)\right]_{\mathcal{R}}$.
(*viii*) Provare che, per ogni $g \in G$, $[g]_{\mathcal{R}} = \{gh \mid h \in H\} = \{g, gB\}$.

Esercizio 3. Siano S un insieme ed A una sua parte. Facendo riferimento all'anello $(\mathcal{P}(S), \triangle, \cap)$, si consideri l'applicazione

$$\varphi_A \colon X \in \mathcal{P}(S) \longmapsto A \triangle X \in \mathcal{P}(S).$$

(*i*) Dimostrare che φ_A è biettiva e determinare φ_A^{-1} (ricordare che A è dotato di opposto in $\mathcal{P}(S)$).
(*ii*) Per quali scelte di A si ha $\varphi_A = \mathrm{id}_{\mathcal{P}(S)}$?

Definita la relazione binaria Σ in $\mathcal{P}(S)$ ponendo, per ogni $X, Y \in \mathcal{P}(S)$,

$$X \Sigma Y \iff X \triangle A \subseteq Y \triangle A,$$

(*iii*) si provi che Σ è una relazione d'ordine.
(*iv*) Si determinino in $(\mathcal{P}(S), \Sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
(*v*) Per quali cardinalità di S la relazione Σ è totale?
(*vi*) Disegnare il diagramma di Hasse di $(\mathcal{P}(S), \Sigma)$ nel caso in cui $S = \{1, 2\}$ e $A = \{1\}$.

Esercizio 4. Sia $f = x^4 - 4x^2 - 21 \in \mathbb{Z}[x]$.

(*i*) Dimostrare che esistono $a, b \in \mathbb{Z}$ tali che $f = (x^2 + a)(x^2 + b)$.
(*ii*) Per ciascuna scelta di A tra i campi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_2$ $\mathbb{Z}_3$, $\mathbb{Z}_5$, riguardato f come polinomio a coefficienti in A, se ne determini una decomposizione in prodotto di polinomi monici irriducibili in $A[x]$ e si dica se f ha o meno radici in A.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
22 MARZO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dare la definizione di *polinomio irriducibile* a coefficienti in un campo.
Il polinomio $f = (x^2+1)(x^2+2)$ è irriducibile in $\mathbb{Q}[x]$?

Esercizio 2. Dati $S = \{1,2,3,4,5\}$ e $T = \{1,2,3\}$, si determini il numero delle applicazioni costanti da S a T, quello delle applicazioni iniettive da S a T, quello delle applicazioni iniettive da T a S.

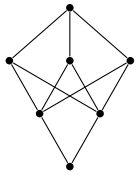
Esercizio 3. Si considerino l'applicazione $f\colon (x,y) \in \mathbb{Z}\times\mathbb{Z} \mapsto xy+1 \in \mathbb{Z}$ ed il suo nucleo di equivalenza $\sim$.

(*i*) f è iniettiva?
(*ii*) f è suriettiva?
(*iii*) Determinare le coppie $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ tali che $|[(x,y)]_\sim| = 2$ e quelle tali che $|[(x,y)]_\sim| = 4$.
(*iv*) Descrivere in modo esplicito $[(0,7)]_\sim$.
(*v*) Provare che, per ogni $n \in \mathbb{Z}\smallsetminus\{0\}$ si ha: $(\forall m \in \mathbb{Z})\big((1,m) \in [(1,n)]_\sim \iff n = m\big)$. Determinare quindi un sottoinsieme A di $\mathbb{Z}\times\mathbb{Z}$ tale che l'applicazione $g\colon (x,y) \in A \mapsto xy+1 \in \mathbb{Z}$ sia biettiva, calcolandone poi l'inversa.

Sia ora σ la relazione d'ordine definita in $\mathbb{Z}\times\mathbb{Z}$ da: $\forall a,b \in \mathbb{Z}\times\mathbb{Z}$

$$a\ \sigma\ b \iff \big(a = b \vee f(a) < f(b)\big).$$

(*vi*) Si determinino in $(\mathbb{Z}\times\mathbb{Z},\sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
(*vii*) $(\mathbb{Z}\times\mathbb{Z},\sigma)$ è totalmente ordinato?
(*viii*) Si determini una parte X di $\mathbb{Z}\times\mathbb{Z}$ tale che (X,σ) sia rappresentata dal diagramma di Hasse disegnato a destra.
(*ix*) (X,σ) è un reticolo?
(*x*) Esiste $a \in X$ tale che $(X\smallsetminus\{a\},\sigma)$ sia un reticolo? Nel caso, indicare un tale a.



Esercizio 4. Si definiscano le due operazioni binarie $\oplus$ e $\circ$ in $\mathbb{Z}_{23}$ ponendo, per ogni $a,b \in \mathbb{Z}_{23}$:

$$a \oplus b = a+b+\bar{1}; \qquad a \circ b = ab+a+b.$$

(*i*) Verificare che $(\mathbb{Z}_{23},\oplus,\circ)$ è un anello commutativo unitario.
(*ii*) Determinarne gli elementi invertibili. $(\mathbb{Z}_{23},\oplus,\circ)$ è un campo?
(*iii*) Se possibile, calcolare l'inverso di $\bar{6}$ in $(\mathbb{Z}_{23},\oplus,\circ)$.
(*iv*) Sia $V = \{-\bar{2},\bar{0}\} \subseteq \mathbb{Z}_{23}$. V è una parte chiusa in $(\mathbb{Z}_{23},\circ)$? V è un sottoanello di $(\mathbb{Z}_{23},\oplus,\circ)$?

Esercizio 5.

(*i*) Verificare che ogni polinomio $f \in \mathbb{Z}_5[x]$ che ammetta $\bar{2}$ e $\bar{4}$ come radici è divisibile per $x^2-x+\bar{3}$.
(*ii*) Scrivere tutti i polinomi in $\mathbb{Z}_5[x]$ che siano di grado 4, prodotto di quattro polinomi monici irriducibili e che ammettano come radici solo $\bar{2}$ e $\bar{4}$. Quanti sono questi polinomi?

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
12 MAGGIO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero).* **Non è necessario consegnare la traccia.**

Esercizio 1. Dato un intero a, dire per quali interi b sono definiti quoziente e resto nella divisione di a per b, enunciando il corrisponente teorema. Chiarire se quoziente e resto sono determinati in modo unico. Fornire quoziente e resto

(*i*) nella divisione di 32 per 7; e
(*ii*) nella divisione di -32 per -7.

Esercizio 2. Sia $\mathbb{P}$ l'insieme dei numeri interi positivi primi e, per ogni $n \in \mathbb{N}$ tale che $n > 1$, siano $\alpha_n = \max\{i \in \mathbb{N}^* \mid (\exists p \in \mathbb{P})(p^i | n)\}$ e $B_n = \{p \in \mathbb{P} \mid p^{\alpha_n} | n\}$. Trovare α_{700} e B_{700}.

Esercizio 3. Posto $S = \{1, 2, 3, 4, 5\}$, si consideri l'applicazione

$$f\colon (a_1, a_2, a_3, a_4, a_5) \in S^5 \longmapsto \{a_1, a_2, a_3, a_4, a_5\} \in \mathcal{P}(S) \setminus \{\varnothing\}$$

ed il nucleo di equivalenza $\mathcal{R}$ di f.

(*i*) f è iniettiva?
(*ii*) f è suriettiva?
(*iii*) Quanti elementi ha l'insieme quoziente $S^5/\mathcal{R}$?
(*iv*) Quanti elementi ha la classe $[(1, 1, 1, 1, 3)]_{\mathcal{R}}$?

Sia σ la relazione d'ordine definita in S^5 ponendo, per ogni $(a_1, a_2, a_3, a_4, a_5), (b_1, b_2, b_3, b_4, b_5) \in S^5$,

$$(a_1, a_2, a_3, a_4, a_5)\ \sigma\ (b_1, b_2, b_3, b_4, b_5) \iff (\forall i \in \{1, 2, 3, 4, 5\})(a_i \leq b_i).$$

(*v*) Si determinino in (S^5, σ) gli eventuali elementi minimali, massimali, minimo, massimo.
(*vi*) Posto $X = \{(1, 1, 5, 2, 3), (1, 2, 4, 3, 5)\}$, si determinino i maggioranti ed i minoranti di X in (S^5, σ), e poi, se esistono, $\inf X$ e $\sup X$.
(*vii*) Provare che, per ogni $\underline{a} = (a_1, a_2, a_3, a_4, a_5), \underline{b} = (b_1, b_2, b_3, b_4, b_5) \in S^5$, posto $Y = \{\underline{a}, \underline{b}\}$ si ha

$$\inf Y = (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \min\{a_3, b_3\}, \min\{a_4, b_4\}, \min\{a_5, b_5\}).$$

(*viii*) (S^5, σ) è un reticolo? È un reticolo booleano?

Esercizio 4. Per ogni intero positivo m si definisca l'operazione binaria $*$ in $\mathbb{Z}_m$ ponendo, per ogni $a, b \in \mathbb{Z}_m$, $a * b = \overline{3}ab$.

(*i*) Verificare che per ogni scelta di m, $(\mathbb{Z}_m, *)$ è un semigruppo commutativo.
(*ii*) Verificare che se $m = 16$ allora $(\mathbb{Z}_m, *)$ è un monoide, individuandone l'elemento neutro e l'insieme degli invertibili.
(*iii*) Trovare, se possibile, l'inverso di $\overline{5}$ in $(\mathbb{Z}_{16}, *)$.
(*iv*) Determinare una parte S di $\mathbb{Z}_{16}$ che sia chiusa rispetto a $*$ e tale che $|S| > 1$.
(*v*) Caratterizzare gli interi positivi m tali che $(\mathbb{Z}_m, *)$ sia un monoide.

Esercizio 5.

(*i*) Determinare in $\mathbb{Q}[x]$ un polinomio f di grado 25 che sia prodotto di tre polinomi irriducibili e che abbia 1 e 2 come uniche radici in $\mathbb{Q}$.
(*ii*) Provare che, comunque un tale f sia stato scelto, esso deve avere in $\mathbb{R}$ almeno una radice non razionale.
(*iii*) Fattorizzare in prodotto di polinomi irriducibili monici il polinomio $x^4 - 14^2$ in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_5[x]$ e $\mathbb{Z}_3[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
21 GIUGNO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *partizione* di un insieme. Siano

$$F_1 = \big\{\{1\},\{2,3\},\{1,4\}\big\}, \qquad F_2 = \big\{1,\{3,4\},\{2\}\big\}, \qquad F_3 = \big\{\{1\},\{4\},\{2,3\}\big\}.$$

Decidere quali tra F_1, F_2 e F_3 sono partizioni di $S := \{1,2,3,4\}$ e, per ciascuna di esse, elencare gli elementi del sottoinsieme di $S \times S$ che descrive la corrispondente relazione di equivalenza in S.

Esercizio 2. Per ogni intero positivo m, si definisca l'operazione binaria $*$ in $A = \mathbb{Z}_6 \times \mathbb{Z}_7$ ponendo, per ogni $(a,b),(c,d) \in A$,

$$(a,b) * (c,d) = (\bar{m}ac, \hat{m}bd)$$

(scriviamo, per ogni $n \in \mathbb{Z}$, $\bar{n}$ per $[n]_6$ e $\hat{n}$ per $[n]_7$). Dando per noto che $*$ è associativa e commutativa,

(*i*) caratterizzare gli $m \in \mathbb{N}^*$ tali che $(A,*)$ sia un monoide.

Si fissi il minimo intero m maggiore di 1 tale che $(A,*)$ sia un monoide. Per questa scelta di m:

(*ii*) determinare l'elemento neutro e gli elementi invertibili di $(A,*)$.

(*iii*) Trovare un elemento $(a,b) \in A$ che non sia né $(\bar{0},\hat{0})$ né l'elemento neutro di $(A,*)$ e tale che $(a,b)^2 = (a,b) * (a,b) = (a,b)$. Esiste un tale (a,b) che sia anche invertibile?

(*iv*) Costruire una parte chiusa X di $(A,*)$ tale che $|X| = 2$ e $(\bar{0},\hat{0}) \notin X$.

Esercizio 3. Sia S l'insieme dei polinomi monici f di secondo grado in $\mathbb{Z}_3[x]$ tali che $f(\bar{0}) = \bar{1}$.

(*i*) Elencare gli elementi di S e scrivere ciascuno di essi come prodotto di polinomi irriducibili monici.

(*ii*) Trovare, se possibile, un esempio di polinomio monico g di grado 4 in $\mathbb{Z}_3[x]$ che sia riducibile, privo di radici e tale che $g(\bar{0}) = \bar{1}$.

Esercizio 4. Sia $Y = \{n \in \mathbb{N} \mid n > 1\}$ e si consideri l'applicazione $f\colon Y \to Y$ che ad ogni $n \in Y$ associa la somma dei numeri primi positivi divisori di n (vale a dire: se $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_r^{\lambda_r}$, dove i p_i sono primi positivi a due a due distinti e, per ogni $i \in \{1,2,\dots,r\}$, $\lambda_i \in \mathbb{N}^*$, allora $f(n) = p_1 + p_2 + \cdots + p_r$). Sia $\sim$ il nucleo di equivalenza di f.

(*i*) f è iniettiva?

(*ii*) f è suriettiva?

(*iii*) Elencare gli elementi di $[9]_\sim$ e quelli di $[5]_\sim$.

Sia σ la relazione d'ordine definita in Y ponendo, per ogni $a,b \in Y$,

$$a \;\sigma\; b \iff (a = b \vee f(a) < f(b)).$$

(*iv*) σ è totale?

(*v*) Caratterizzare, per ogni $x \in Y$, l'insieme degli elementi di Y non confrontabili con x.

(*vi*) Determinare in (Y,σ) gli eventuali elementi minimali, massimali, minimo, massimo.

(*vii*) Descrivere i minoranti e i maggioranti di $X = \{5,6\}$ e individuare, se esistono (o spiegare perché non esistono) $\inf X$ e $\sup X$ in (Y,σ).

(*viii*) (Y,σ) è un reticolo?

(*ix*) Costruire due sottoinsiemi C e D di Y, entrambi di cardinalità 8, tali che:

- (C,σ) sia un reticolo complementato ma non distributivo;
- (D,σ) sia un reticolo distributivo ma non complementato né totalmente ordinato.

[Suggerimento: disegnare prima i diagrammi di Hasse dei reticoli che si intendono costruire.]

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
10 LUGLIO 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di reticolo *complementato*.

Esercizio 2. Per ciascuna delle uguaglianze qui elencate caratterizzare gli interi m per i quali essa si verifica.

(*i*) $[3]_m + [5]_m = [17]_m$;
(*ii*) $[3]_m \cdot [5]_m = [3]_m - [5]_m$;
(*iii*) $[3]_m \cdot [5]_m = [1]_m$;
(*iv*) $[5]_m = [3]_m^{-1}$.

Esercizio 3. Sia S un insieme.

(*i*) $(\mathcal{P}(S), \triangle)$ è un gruppo abeliano; qual è il suo elemento neutro?
(*ii*) E se $X \in \mathcal{P}(S)$, qual è il simmetrico di X in $(\mathcal{P}(S), \triangle)$?
(*iii*) Quali elementi di $\mathcal{P}(S)$ sono cancellabili rispetto a $\triangle$? E quali rispetto a $\cup$?

Ricordando questi risultati, fissato un $A \in \mathcal{P}(S)$, si consideri l'operazione binaria $*$ in $\mathcal{P}(S)$ definita da: per ogni $X, Y \in \mathcal{P}(S)$,

$$X * Y = X \triangle Y \triangle A.$$

(*iv*) $*$ è associativa? È commutativa?
(*v*) $(\mathcal{P}(S), *)$ ha elemento neutro? Se lo ha, quali sono i suoi elementi simmetrizzabili?
(*vi*) Se $A \neq \varnothing$ e $a \in A$, l'insieme $B = \{X \in \mathcal{P}(S) \mid a \in X\}$ è chiuso rispetto a $*$?

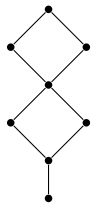
Esercizio 4. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{Z} \times \mathbb{Z} \to a + b^2 \in \mathbb{Z}$; sia $\sim$ il suo nucleo di equivalenza.

(*i*) f è iniettiva?
(*ii*) f è suriettiva?
(*iii*) Descrivere esplicitamente gli elementi di $[(0, 0)]_\sim$.
(*iv*) Verificare: $(\forall b \in \mathbb{Z})(\exists! a \in \mathbb{Z})((a, b) \in [(1, 0)]_\sim)$, descrivendo in modo esplicito un tale a in dipendenza da b.

Sia σ la relazione d'ordine definita in $\mathbb{N} \times \mathbb{N}$ ponendo, per ogni $x, y \in \mathbb{N} \times \mathbb{N}$,

$$x \,\sigma\, y \iff (x = y \vee f(x) < f(y)).$$

(*v*) Determinare in $(\mathbb{N} \times \mathbb{N}, \sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
(*vi*) Descrivere i minoranti e i maggioranti di $X = \{(0, 1), (1, 0)\}$ e individuare, se esistono (o spiegare perché non esistono) $\inf X$ e $\sup X$ in $(\mathbb{N} \times \mathbb{N}, \sigma)$.
(*vii*) $(\mathbb{N} \times \mathbb{N}, \sigma)$ è un reticolo?
(*viii*) Sia $Y = \{(0, 0), (0, 1), (1, 0), (0, 3), (5, 2), (5, 3)\}$. Disegnare il diagramma di Hasse di (Y, σ) e stabilire se questo è un reticolo. Nel caso, (Y, σ) è distributivo? È complementato?
(*ix*) Trovare un sottoinsieme W di $\mathbb{N} \times \mathbb{N}$ tale che $|W| = 8$ e (W, σ) abbia il diagramma di Hasse disegnato a destra. Decidere se (W, σ) è un reticolo e se è isomorfo a $(\mathcal{P}(S), \subseteq)$ per qualche insieme S di cardinalità 3.



Esercizio 5. Determinare l'insieme T dei primi p tali che il polinomio $f_p = x^3 - x^2 + \bar{2}x + \bar{1} \in \mathbb{Z}_p[x]$ ammetta $-\bar{2}$ come radice. Per ogni $p \in T$, scrivere f_p come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
5 SETTEMBRE 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

Esercizio 1. Siano n e k due numeri naturali e sia A un insieme di cardinalità n. Assumendo $k \leq n$, quale tra questi tre numeri è $|\{B \subseteq A \mid |B| = k\}|$?

$$n!/k!; \qquad \binom{n}{k}; \qquad n!/(n-k)!.$$

Se $|A| = 10$, quanti sono:

(i) i sottoinsiemi di A di cardinalità 3?
(ii) quelli di cardinalità 7?
(iii) le applicazioni iniettive da $\{1, 2, 3\}$ ad A?

Esercizio 2. Studiare le due equazioni congruenziali

$$\text{(A)}\colon 18x \equiv_{62} 13 \qquad \text{e} \qquad \text{(B)}\colon 18x \equiv_{62} 14,$$

determinando per ciascuna di esse l'insieme di *tutte* le soluzioni intere.

Esercizio 3. Sia $S = \{0, 1, 2, 3, 4, 5\}$. Esiste una ed una sola relazione di equivalenza $\sim$ in S tale che $\{2, 3\} \subseteq [0]_\sim$, $1 \sim 4$ e $|S/\!\sim| = 3$.

(i) Descrivere $S/\!\sim$ elencando gli elementi di ciascuna classe di equivalenza rispetto a $\sim$.

Si consideri l'applicazione $f\colon a \in S \mapsto [a]_\sim \in \mathcal{P}(S)$.

(ii) f è iniettiva? f è suriettiva?
(iii) Vero o falso (e perché): $\sim$ è il nucleo di equivalenza di f.

Esercizio 4. Si consideri la relazione d'ordine σ definita in $\mathbb{N} \times \mathbb{N}$ ponendo, per ogni $a, b, c, d \in \mathbb{N}$,

$$(a, b)\ \sigma\ (c, d) \iff (a \leq c \wedge b|d).$$

(i) Determinare in $(\mathbb{N} \times \mathbb{N}, \sigma)$ gli eventuali elementi minimali, massimali, minimo, massimo.
(ii) Elencare i minoranti e descrivere i maggioranti in $(\mathbb{N} \times \mathbb{N}, \sigma)$ di $X = \{(2, 14), (5, 21)\}$ e individuare, se esistono, (o spiegare perché non esistono) $\inf X$ e $\sup X$ in $(\mathbb{N} \times \mathbb{N}, \sigma)$.
(iii) Trovare, se possibile, due sottoinsiemi B e C di $\mathbb{N} \times \mathbb{N}$ tali che $|B| = |C| = 4$ e
  (a) (B, σ) sia un reticolo booleano;
  (b) (C, σ) sia totalmente ordinato.

Sia $T = \{(1, 1), (1, 2), (1, 3), (1, 5), (1, 60), (2, 0), (2, 5)\}$.

(iv) Disegnare il diagramma di Hasse di (T, σ), stabilendo se questo è un reticolo, un reticolo distributivo, un reticolo complementato.
(v) Esiste $y \in \mathbb{N} \times \mathbb{N}$ tale che $(T \cup \{y\}, \sigma)$ sia un reticolo booleano?

Esercizio 5.

(i) Sia $f = (x^3 + \bar{1})(x^3 - x + \bar{1}) \in \mathbb{Z}_3[x]$. Dopo aver calcolato $f(-\bar{1})$, si decomponga f in prodotto di polinomi irriducibili monici.
(ii) Sempre in $\mathbb{Z}_3[x]$, si consideri l'operazione binaria $*$ definita ponendo, per ogni $g, h \in \mathbb{Z}_3[x]$, $g * h = g^2 + h$.
  (a) $*$ è commutativa? $*$ è associativa?
  (b) $(\mathbb{Z}_3[x], *)$ ha elementi neutri a sinistra, neutri a destra, neutri?
  (c) L'insieme $\{xg \mid g \in \mathbb{Z}_3[x]\}$ è una parte chiusa in $(\mathbb{Z}_3[x], *)$?

CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
16 OTTOBRE 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

Esercizio 1. Sia F un campo. Si dica quando due polinomi non nulli f e g in $F[x]$ sono *associati*. Inoltre:

(*i*) Vero o falso (e perché): due polinomi non nulli in $F[x]$ sono associati se e solo se hanno lo stesso grado.

(*ii*) Si elenchino i polinomi associati a $\bar{2}x^2 + \bar{1}$ in $\mathbb{Z}_5[x]$.

Esercizio 2. Vero o falso? E perché?

(*i*) Per ogni relazione d'ordine σ in $\mathbb{N}$ si ha: $(\forall a \in \mathbb{N})(\exists b \in \mathbb{N})(b \neq a \wedge a\ \sigma\ b)$.

Per ogni insieme ordinato $(S, \leq)$,

(*ii*) se a è l'unico elemento minimale di $(S, \leq)$, allora $a = \min S$;

(*iii*) se $a = \min S$, allora a è l'unico elemento minimale di $(S, \leq)$;

(*iv*) se esiste $\inf S$, allora $\inf S = \min S$.

Se, inoltre, $(S, \leq)$ è un reticolo,

(*v*) esistono $\inf S$ e $\sup S$;

(*vi*) gli elementi di S sono a due a due confrontabili;

(*vii*) se $(S, \leq)$ è complementato, $(\forall x, y \in S)(x \wedge y = \min S \text{ e } x \vee y = \max S)$.

Esercizio 3. Quali tra i seguenti sono diagrammi di Hasse di un insieme ordinato? Quali tra questi rappresentano un reticolo?

(1) (2) (3) (4) (5)

Riguardate le stesse cinque figure come grafi, dire quali rappresentano alberi e individuare le coppie che rappresentano grafi tra loro isomorfi.

Esercizio 4. Considerate le applicazioni $\varphi\colon a \in \mathbb{Z}_{25} \mapsto \bar{3}a \in \mathbb{Z}_{25}$ e $\psi\colon a \in \mathbb{Z}_{25} \mapsto \overline{15}a \in \mathbb{Z}_{25}$,

(*i*) verificare che φ è biettiva, calcolandone l'inversa;

(*ii*) verificare che nessun elemento invertibile di $(\mathbb{Z}_{25}, \cdot)$ appartiene all'immagine di ψ;

Esercizio 5. Sia A un insieme. In $T := \mathcal{P}(A) \times \mathcal{P}(A) \times \mathcal{P}(A)$ si definisca l'operazione binaria $*$ ponendo, per ogni $X, Y, Z, \bar{X}, \bar{Y}, \bar{Z} \in \mathcal{P}(A)$, $(X, Y, Z) * (\bar{X}, \bar{Y}, \bar{Z}) = (X \cup \bar{X}, Y \cap \bar{Y}, Z \triangle \bar{Z})$.

(*i*) Provare (facendo uso di proprietà insiemistiche note) che $(T, *)$ è un monoide, specificandone l'elemento neutro;

(*ii*) determinare gli elementi invertibili di $(T, *)$;

(*iii*) verificare che, per ogni $X \in \mathcal{P}(A)$, $T_X := \{(X, X, Z) \mid Z \in \mathcal{P}(A)\}$ è una parte chiusa in $(T, *)$ e che $(T_X, *)$ è un gruppo.

Esercizio 6. Per quali primi positivi p il polinomio $f_p = \overline{30}x^5 + x^3 + \bar{2}x + \bar{2} \in \mathbb{Z}_p[x]$ ha grado 3?

(*i*) Per ciascuno di tali primi p, scrivere f_p come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$.

(*ii*) Il polinomio $x^3 + 2x + 2$ è irriducibile in $\mathbb{R}[x]$? Ha radici in $\mathbb{R}$?

CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
13 NOVEMBRE 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.
Non è necessario consegnare la traccia.

Esercizio 1. Definire la nozione di classe di equivalenza.

Vero o falso? E perché? Per ogni insieme A ed ogni relazione di equivalenza $\sim$ in A:

(*i*) $(\forall a, b \in A)([a]_\sim \cap [b]_\sim \neq \varnothing \Rightarrow a \sim b)$.
(*ii*) $(\forall a, b \in A)(a \sim b \Rightarrow [a]_\sim = [b]_\sim)$.
(*iii*) Se A è finito, $A/\!\sim$ è finito.
(*iv*) Se A è infinito, $A/\!\sim$ è infinito.

Siano $S = \{1, 2, 3\}$ e $T = \{n \in \mathbb{N} \mid n < 10\}$.

(*v*) Quante sono le relazioni di equivalenza in S?
(*vi*) Esiste una relazione di equivalenza σ in T tale che $T/\sigma = \big\{\{0, 3, 4\}, \{1, 8\}, \{2, 5, 6, 7\}, \{9\}\big\}$?

Sia ora α la relazione di equivalenza in $X = \{0, 1, 2, 3, 4, 5\}$ definita da

$$(\forall x, y \in X)\big(x\ \alpha\ y \iff x^2 \equiv_3 (2y)^2\big).$$

(*vii*) Elencare gli elementi di ciascuna delle classi di equivalenza modulo α e descrivere X/α, indicando quanti elementi ha.

Esercizio 2. Sia f l'applicazione $(a, b) \in \mathbb{Q} \times \mathbb{Q} \mapsto a(a + 2b) \in \mathbb{Q}$.

(*i*) f è suriettiva? f è iniettiva?
(*ii*) Determinare $[(0, 0)]_\rho$, dove ρ è il nucleo di equivalenza di f.
(*iii*) Determinare le coppie $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tali che $f(a, b) = -1$.
(*iv*) Per ogni numero primo dispari p, determinare le coppie $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tali che $f(a, b) = p$.

Esercizio 3. Si consideri in $\mathbb{Z}$ la relazione d'ordine σ definita da:

$$(\forall a, b \in \mathbb{Z})\big(a\ \sigma\ b \iff (a = b \vee \mathrm{rest}(a, 5) < \mathrm{rest}(b, 5))\big).$$

(*i*) Determinare in $(\mathbb{Z}, \sigma)$ gli insiemi degli elementi minimali e massimali, rappresentandoli se possibile come unioni di classi di resto. Determinare in $(\mathbb{Z}, \sigma)$ gli eventuali minimo e massimo.
(*ii*) Determinare in $(\mathbb{Z}, \sigma)$, per ciascuno di $X = \{6, -4\}$ e $Y = \{6, 2\}$:
  (a) gli insiemi di minoranti e dei maggioranti, rappresentandoli se possibile come unioni di classi di resto;
  (b) gli eventuali estremi inferiori e superiori.
(*iii*) $(\mathbb{Z}, \sigma)$ è un reticolo?
(*iv*) Sia $S = \{0, 1, 2, 3, 4, 6, 13, 23\}$. (S, σ) è un reticolo? Quali condizioni (necessarie e sufficienti) deve verificare un $a \in \mathbb{Z}$ affinché $(S \cup \{a\}, \sigma)$ sia un reticolo?

Esercizio 4. Nell'anello $(M_2(\mathbb{Z}_{10}), +, \cdot\,)$ delle matrici 2×2 su $\mathbb{Z}_{10}$ (dove $+$ e $\cdot$ indicano le consuete operazioni di addizione e di moltiplicazione righe per colonne tra matrici), si consideri la parte $T = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \,\middle|\, a, b, c \in \mathbb{Z}_{10} \right\}$.

(*i*) Si provi che T è chiusa rispetto a $+$ e $\cdot$ e, sfruttando le già note proprietà delle operazioni tra matrici, che $(T, +, \cdot\,)$ è un anello unitario non commutativo.
(*ii*) Determinare gli elementi invertibili di T (rispetto a $\cdot$). Quanti sono?
(*iii*) Facendo uso di un'opportuna equazione congruenziale, scrivere l'inverso di $\left(\begin{smallmatrix} \bar{3} & \bar{1} \\ \bar{0} & \bar{7} \end{smallmatrix}\right)$ in T.

Esercizio 5. Per ogni primo p si considerino i polinomi $f_p = \bar{2}x^2 + \bar{3}x + \bar{1}$ e $g_p = \bar{3}x^2 - \bar{4}x + \bar{2}$ in $\mathbb{Z}_p[x]$.

(*i*) Per quali primi p il polinomio $f_p g_p$ è monico?
(*ii*) Detto q il massimo tale primo, scrivere $f_q g_q$ come prodotto di polinomi irriducibili in $\mathbb{Z}_q[x]$.

CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
12 DICEMBRE 2017

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.
Non è necessario consegnare la traccia.

Esercizio 1. Si diano le definizioni di *anello* e di *campo*.
In $\mathbb{Q}$ si considerino le operazioni binarie $\oplus$ e $*$ definite ponendo, per ogni $a, b \in \mathbb{Q}$,

$$a \oplus b = a + b + 1 \qquad \text{e} \qquad a * b = ab + a + b.$$

(*i*) Dando per noto che $\oplus$ e $*$ sono commutative e associative, provare che $(\mathbb{Q}, \oplus, *)$ è un anello commutativo unitario. $(\mathbb{Q}, \oplus, *)$ è un campo?
(*ii*) Stabilire se $3\mathbb{Z}$ è una parte chiusa di $\mathbb{Q}$ rispetto a $\oplus$ e se lo è rispetto a $*$.

Esercizio 2. Siano S e T insiemi. Assumendo $|S| = 3$ e $|T| = 5$ calcolare:
(*i*) il numero delle applicazioni iniettive da S a T;
(*ii*) il numero delle applicazioni iniettive da T a S;
(*iii*) il numero delle applicazioni suriettive da S a T;
(*iv*) il numero delle applicazioni da S a T;
(*v*) il numero delle applicazioni costanti da S a T.

Sia poi $f\colon S \to T$ un'applicazione e sia $\mathcal{R}_f$ il suo nucleo di equivalenza. Determinare $\mathcal{R}_f$ e calcolare $S/\mathcal{R}_f$ in ciascuno dei due casi:
(*vi*) f è iniettiva;
(*vii*) f è costante.

Esercizio 3. Esiste in $\mathbb{Z}_{54}$ una classe a tale che $\overline{20}a = \bar{4}$? Ed esiste una classe b tale che $\overline{20}b = \bar{5}$? In entrambi i casi, fornire se possibile almeno un esempio.

Esercizio 4. Sia A l'insieme dei numeri interi maggiori di 1. Per ogni $n \in A$, sia p_n il massimo primo positivo divisore di n. Definiamo in A la relazione binaria σ ponendo, per ogni $a, b \in A$:

$$a \;\sigma\; b \iff \big(p_a < p_b \vee (p_a = p_b \wedge a \leq b)\big)$$

(*i*) σ è una relazione d'ordine? Nel caso lo sia, rispondere anche alle domande che seguono.
(*ii*) Determinare in (A, σ) gli eventuali minimo, massimo, elementi minimali, elementi massimali.
(*iii*) (A, σ) è totalmente ordinato? È un reticolo?
(*iv*) Posto $B = \{3^n \mid n \in \mathbb{N}^*\}$, determinare in (A, σ) gli insiemi dei minoranti e dei maggioranti di B e, se esistono, $\inf B$ e $\sup B$.

Esercizio 5.
(*i*) Determinare quanti sono e che forma hanno i polinomi $f \in \mathbb{Z}_5[x]$ che siano monici di grado 5 e tali che $f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = \bar{0}$.
(*ii*) Tra questi polinomi, dire se esistono, e nel caso quanti sono e che forma hanno, quelli che siano prodotto di cinque fattori irriducibili, di tre fattori irriducibili, di due fattori irriducibili.
(*iii*) Scrivere $g = x^5 - x \in \mathbb{Z}_5[x]$ come prodotto di polinomi irriducibili monici.
(*iv*) Spiegare perché ogni polinomio $f \in \mathbb{Z}_5[x]$ tale che $f(a) = \bar{0}$ per ogni $a \in \mathbb{Z}_5$ è multiplo di g.