Esercizi algebra 2 9-11-10

(1) Sia A l'anello $\mathbb{Z}[\sqrt{-6}]$ e $N : A \mapsto \mathbb{Z}$ la norma definita da $N(a + b\sqrt{-6}) = a^2 + 6b^2$. Provare che:
  (a) non esistono elementi in A di norma 2 o 5;
  (b) gli elementi $2,\ 5,\ 2 + \sqrt{-6}$ sono irriducibili ma non primi.
  (c) Dedurre dai punti precedenti che A non e' un domino a fattorizzazione unica e trovare un elemento con due fattorizzazioni diverse.

(2) Sia $\mathbb{F}$ campo. Provare che in $\mathbb{F}[x, y]$ gli elementi x e y hanno massimo comun divisore ma non soddisfano un'identita' di Bezout.

(3) Provare che gli elementi 9 e $6 + 3\sqrt{-5}$ non ammettono MCD in $\mathbb{Z}[\sqrt{-5}]$.

(4) Sia $R = \mathbb{Z}[2i] = \{a + 2bi \mid a,\ b \in \mathbb{Z}\}$ sottoanello degli interi di Gauss. Si provi che:
  (a) R è un dominio d'integrita';
  (b) gli elementi 2 e $2i$ sono irriducibili ma non associati in R
  (c) R non è un dominio a fattorizzazione unica;
  (d) il campo dei quozienti di R è $\mathbb{Q}[i]$.
  (e) il polinomio $p(x) = x^2 + 1$ è riducibile in $\mathbb{Q}[i][x]$ ma è irriducibile in $R[x]$.

(5) Sia D domino d'integrita', Q il suo campo dei quozienti e i l'iniezione canonica di D in Q. Se $\psi : D \to F$ e' un omomorfismo iniettivo in un campo F allora esiste un unico omomorfismo iniettivo $\bar{\psi} : Q \to F$ tale che $\bar{\psi} \circ i = \psi$.

(6) Si descrivano le classi di coniugio del gruppo simmetrico S_5 e di ogniuna se ne calcoli la cardinalita'.

(7) Si calcoli la cardinalita' della classe di coniugio di $(1, 2)(3, 4)(5, 6)(7, 8, 9)(10, 11, 12)$ in S_{15}.

(8) Si trovi una formula per calcolare il numero di coniugati di un elemento in S_n data una sua scomposizione in cicli disgiunti.

(9) Classificazione degli elementi primi di $\mathbb{Z}[i]$.
  (a) Sia $\pi = a + ib \in \mathbb{Z}[i]$ tale che $N(\pi) = a^2 + b^2 = p$ è primo in $\mathbb{Z}$. Allora π è primo in $\mathbb{Z}[i]$.
  (b) Sia $p \in \mathbb{N}$ un primo con $p \equiv 1 \mod 4$, diciamo $p = 4n + 1$, allora $x = (2n)!$ è soluzione di $x^2 \equiv -1 \mod p$.
  (c) Se $p \in \mathbb{N}$ è un primo tale che $p \equiv 1 \mod 4$, allora p è riducibile in $\mathbb{Z}[i]$ ed e' somma di due quadrati univocamente determinati.
  (d) Se $p \in \mathbb{N}$ è un primo tale che $p \equiv 3 \mod 4$, allora p è primo in $\mathbb{Z}[i]$.
  (e) Sia $\pi \in \mathbb{Z}[i]$ un primo tale che $\pi \notin \mathbb{Z},\ i\mathbb{Z}$, allora $N(\pi) = 2$ oppure $N(\pi) = p$ dove $p \equiv 1 \mod 4$ è un primo.
  (f) Dedurre la classificazione dei primi di $\mathbb{Z}[i]$ dai punti precedenti.