Prof. Lidia Angeleri, Prof. Francesca Mantese
Università di Verona, 2012/2013
Corso di Laurea in Matematica Applicata

Esercizi per il Corso di ALGEBRA

Foglio 5
31 ottobre 2012

1. Si consideri il polinomio $f = x^4 + x^3 + x^2 + 2x + 3$ in $\mathbb{Z}/5\mathbb{Z}[x]$
   (a) Si scriva f come prodotto di irriducibili in $\mathbb{Z}/5\mathbb{Z}[x]$
   (b) Sia $R = \frac{\mathbb{Z}/5\mathbb{Z}[x]}{(f)}$. Si dica se $x^2 + 1 + (f)$ è divisore di zero in R.
   (c) Si verifichi che $x - 1 + (f)$ è invertibile in R e se ne trovi l'inverso

   (8 punti)

2. Sia $\tilde{R} = \mathbb{Z}[i\sqrt{3}] = \{a + i\sqrt{3}\, b \,|\, a, b \in \mathbb{Z}\}$. Si verifichi:
   (a) $\tilde{R}$ è un sottoanello di $\mathbb{C}$.
   (b) Gli elementi 2, $1 + i\sqrt{3}$, $1 - i\sqrt{3}$ sono elementi irriducibili di $\tilde{R}$.
   (c) L'anello $\tilde{R}$ non è un dominio a fattorizzazione unica (UFD), cioè in $\tilde{R}$ *non* vale l'enunciato del Teorema 8.10.

   (*6 punti*)

3. (a) Si usi l'Algoritmo Euclideo per calcolare il massimo comun divisore d di $a = 1848$ e $b = 980$ e si trovino $\alpha, \beta \in \mathbb{Z}$ tali che $d = \alpha a + \beta b$.
   (b) Si scompongano $a = 1848$ e $b = 980$ in fattori primi e si usi la scomposizione per determinare il massimo comun divisore e il minimo comune multiplo di a e b.

   (4 punti)

4. Sia $F = \frac{\mathbb{Z}/3\mathbb{Z}[x]}{I}$, dove $I = (x^2 + 2x + 2)$.
   (a) Si verifichi che F è un campo
   (b) Quanti elementi ha F?
   (c) l'elemento $x + I$ è un quadrato in F?

   (8 punti)

5. Sia R un dominio. Un elemento $r \in R$ si dice *primo* se $r \mid ab$ implica $r \mid a$ oppure $r \mid b$. Si dimostri che un elemento $r \in R$ è primo se e solo se $R/(r)$ è un dominio di integrità.

   (4 punti)

6. Si consideri l'anello $\mathbb{Z}[i]$ degli interi di Gauss. Sia $p \in \mathbb{Z}$ un numero primo. Si dimostri che le seguenti affermazioni sono equivalenti:

   (a) $p = a^2 + b^2$ dove $a, b \in \mathbb{Z}$

   (b) $p = 2$ oppure $4 \mid p - 1$

   (c) -1 è un quadrato in $\mathbb{Z}/p\mathbb{Z}$

   (d) l'anello $\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}$ non è un dominio

   (e) p non è un elemento irriducibile di $\mathbb{Z}[i]$

   (Sugg: si dimostri $a) \Rightarrow b) \Rightarrow c) \Rightarrow d) \Rightarrow e) \Rightarrow a)$
   per $b) \Rightarrow c)$ si ricordi che gli elementi invertibili di $\mathbb{Z}/p\mathbb{Z}$ formano un gruppo ciclico di ordine $p - 1$.
   per $c) \Rightarrow d)$ si considerino le radici del polinomio $x^2 + 1$ in $\frac{\mathbb{Z}[i]}{p\mathbb{Z}[i]}[x]$ e si ricordi il teorema di Ruffini (e il suo corollario).
   per $d) \Rightarrow e)$ si usi l'esercizio precedente
   per $e) \Rightarrow a)$ a partire da una decomposizione di p in $\mathbb{Z}[i]$ si scriva una decomposizione di p^2 in $\mathbb{Z}$

(**)

Consegna: giovedì 8 novembre durante le esercitazioni.