

Universita' degli Studi di Roma "Tor Vergata"
Laurea Triennale in Matematica - a.a. 2024/2025

Corso: Algebra 1

Docente: Prof.ssa I. Damiani, Codocente: Prof. F. Flamini

Esercitazioni/Tutorati 14 (3 Giugno 2025) - Prof. F. Flamini

Esercizio 1. Sia $\mathbb{Z}[i]$ l'anello degli interi di Gauss

(i) Dato $\alpha := a + bi \in \mathbb{Z}[i]$ con $\text{MCD}(a, b) = 1$ in $\mathbb{Z}$, i.e. a e b interi **coprime**, dimostrare che l'anello quoziente $\frac{\mathbb{Z}[i]}{(a+ib)}$ é isomorfo a $\mathbb{Z}/(a^2 + b^2)\mathbb{Z}$, e pertanto esso é un campo se e solo se la **valutazione** dell'elemento $a + bi \in \mathbb{Z}[i]$ é un numero primo $p \in \mathbb{N}$.

(ii) Preso $\beta = 6 + 3i$ calcolare la **cardinalità** e la **caratteristica** dell'anello quoziente $A := \mathbb{Z}[i]/(6 + 3i)$.

Sviluppare lo svolgimento di (ii) nei seguenti punti intermedi:

- Notare che in $\mathbb{Z}[i]$ l'elemento $6 + 3i$ si fattorizza in $6 + 3i = 3(2 + i)$, ricordando che 3 e $2 + i$ sono irriducibili in $\mathbb{Z}[i]$.
- Notare che $\text{MCD}(3, 2 + i)$ in $\mathbb{Z}[i]$ é un'unità di $\mathbb{Z}[i]$ quindi e' **associato** ad 1 e dunque 3 e $2 + i$ sono **coprime** in $\mathbb{Z}[i]$.
- Detti $I = (3)$ e $J = (2 + i)$ gli ideali in $\mathbb{Z}[i]$ essi sono ideali primi (equivalentemente massimali perché $\mathbb{Z}[i]$ euclideo dunque PID) e sono **ideali coprimi**.
- Dal **Teorema cinese dei resti (versione negli anelli quozienti)** ricordare che $(6 + 3i) = I \cdot J = I \cap J$ e che

$$\frac{\mathbb{Z}[i]}{(6 + 3i)} \simeq \frac{\mathbb{Z}[i]}{I} \times \frac{\mathbb{Z}[i]}{J}$$

prodotto diretto di campi, visto che I e J massimali in $\mathbb{Z}[i]$.

- Ricordare che $\frac{\mathbb{Z}[i]}{I} = \frac{\mathbb{Z}[i]}{(3)}$ é il campo già studiato nell'**Esercitazione 12 - 26 Maggio 2025**, dove si é dimostrato che $\frac{\mathbb{Z}[i]}{(3)} \simeq \frac{(\mathbb{Z}/3\mathbb{Z})[x]}{(x^2+1)}$ e dove avevamo visto che era un campo con 9 elementi.
- Osservare che $\frac{\mathbb{Z}[i]}{J} = \frac{\mathbb{Z}[i]}{(2+i)}$ é un quoziente come nel punto (i), dove $a^2 + b^2 = 5$, perciò é isomorfo a $\mathbb{Z}/5\mathbb{Z}$.
- Dall'isomorfismo $\frac{\mathbb{Z}[i]}{(6+3i)} \simeq \frac{\mathbb{Z}[i]}{I} \times \frac{\mathbb{Z}[i]}{J}$ si deduce quindi la cardinalità di $\frac{\mathbb{Z}[i]}{(6+3i)}$.
- Per determinare la caratteristica di A , ricordare che essa é il **periodo (od ordine) additivo** dell'unità $1_A \in A$, cioè il minimo $n \in \mathbb{N}$ tale che $n \cdot 1_A = 0_A$.

Esercizio 2. Si consideri l'anello dei polinomi $\mathbb{Q}[x, y]$ e si consideri il polinomio $f(x, y) := x^2y^2 + 2x + 2 \in \mathbb{Q}[x, y]$.

(i) Dimostrare che $\mathbb{Q}[x, y]$ é **DFU** e che $f(x, y)$ é **irriducibile** in $\mathbb{Q}[x, y]$.

(ii) Considerato il polinomio $g(x) := x^2 + 2x + 2 \in \mathbb{Q}[x] \subset \mathbb{Q}[x, y]$, dimostrare che l'anello quoziente $B := \mathbb{Q}[x, y]/(g(x))$ é **DFU** dotato di un naturale morfismo suriettivo di domini di integrità

$$\varphi : \mathbb{Q}[x, y] \twoheadrightarrow B$$

dove $\varphi(f(x, y)) \in B$ é **riducibile** in B , trovando i **fattori irriducibili** di $\varphi(f(x, y)) \in B$.

Esercizio 3. (i) Si considerino $a, n \in \mathbb{N} \setminus \{0\} \subset \mathbb{Z}$ interi **coprime** e sia ϕ la **funzione di Eulero**. Dimostrare che

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Dedurre che se $n = p$ primo in $\mathbb{N}$, si ha in particolare che per ogni $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ si ha

$$a^{p-1} \equiv 1 \pmod{p}$$

e che per ogni $a \in \mathbb{Z}/p\mathbb{Z}$ si ha

$$a^p \equiv a \pmod{p}.$$

(ii) Siano $b = 123456$, $k = 987654 \in \mathbb{N}$. Utilizzare opportunamente il punto (i) per determinare $x \in \{0, 1, \dots, 10\}$ per cui

$$b^k = (123456)^{987654} \equiv x \pmod{11}.$$

(iii) Determinare tutte le soluzioni modulo 70 del **sistema di congruenze non lineare**

$$\begin{cases} x^2 \equiv 4 & \pmod{14} \\ x \equiv 3 & \pmod{5} \end{cases}.$$

Esercizio 4. Si consideri il polinomio $f(x, y) \in \mathbb{R}[x, y]$ dato da

$$f(x, y) = y^3 - (x^2 + 1).$$

Un punto $P = (x_0, y_0) \in \mathbb{R}^2 = \mathbb{A}^2(\mathbb{R})$ si dice **soluzione** di $f(x, y)$ se $f(x_0, y_0) = 0$, i.e. se vale

$$y_0^3 = x_0^2 + 1,$$

equivalentemente $P = (x_0, y_0) \in C$ dove C la **curva affine** determinata da

$$C := \{P = (x_0, y_0) \in \mathbb{R}^2 = \mathbb{A}^2(\mathbb{R}) \mid y_0^3 = x_0^2 + 1\}.$$

(i) Stabilire che se (x_0, y_0) é **soluzione intera** di $f(x, y)$, i.e. $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ (equivalentemente P su C é un **punto a coordinate intere**) allora $x_0 \in \mathbb{Z}$ é necessariamente un numero intero pari.

(ii) Se (x_0, y_0) é soluzione intera di $f(x, y)$, stabilire che gli elementi $x_0 + i$, $x_0 - i \in \mathbb{Z}[i]$ sono **coprime** nell'anello degli interi di Gauss $\mathbb{Z}[i]$.

(iii) Dedurre da (ii) e dal fatto che (x_0, y_0) é soluzione intera di $f(x, y)$, che allora gli elementi $x_0 + i$, $x_0 - i \in \mathbb{Z}[i]$ sono **cubi** in $\mathbb{Z}[i]$, i.e. esistono $\alpha := a + ib$, $\beta := a' + ib' \in \mathbb{Z}[i]$ tale che $x_0 + i = \alpha^3$, $x_0 - i = \beta^3$.

(iv) Dedurre da (iii) che $f(x, y)$ ha come unica soluzione intera $(x_0, y_0) = (0, 1)$ (equivalentemente l'unico punto P a coordinate intere su C é $P = (0, 1)$).