Lezione 10 Algebra I

Federico De Sisti

2024-11-02

1 Numeri primi e aritmetica

Definizione 1 (Numero primo)
Un intero $\rho > 1$ si dice primo se $\forall a, b\mathbb{Z}$

$$\rho | ab \rightarrow \rho | a \text{ oppure } \rho | b.$$

Definizione 2 (Numero irriducibile)
Un intero $\rho > 1$ si dice irriducibile se i suoi unici divisori positivi sono 1 e ρ

Esercizio:
Dimostrare che ρ è primo $\Leftrightarrow$ è irriducibile

Teorema 1 (Fondamentale dell'aritmetica)
$n > 1$ intero. Allora n si scrive in modo unico come

$$n = \rho_1^{k_1} \cdot \ldots \cdot \rho_r^{k_r} \qquad \text{(forma canonica)}$$

dove $k_i > 0 \;\; \forall i \in \{1, \ldots, r\}$
e $\rho_1 < \rho_2 < \ldots < \rho_r$
e ρ_i è primo $\forall i \in \{1, \ldots, r\}$

Teorema 2
ρ primo. Allora
$\sqrt{\rho}$ è irrazionale (ovvero $\sqrt{\rho} \ni \mathbb{Q}$)

Dimostrazione (Per assurdo)
$\exists a, b \in \mathbb{Z}$ *t.c.* $\sqrt{\rho} = \frac{a}{b}$ *con* $MCD(a, b) = 1$
Allora:
$(a) + (b) = (MCD(a, b)) = (1)$
$\rightarrow 1 \in (a)) + (b)$
$\exists r, s, \in$, *t.c.* $1 = ra + sb$ *(identità di Bezout)*
ora: $\begin{cases} a = \sqrt{\rho} b \\ b\rho = a\sqrt{\rho} \end{cases}$
Quindi: $\sqrt{\rho} = \rho \cdot 1 = \sqrt{\rho} \cdot (ra + sb)$
$(\sqrt{\rho} a)r + (\sqrt{\rho} b)s$
$= \rho br + as \in \mathbb{Z}$
$\Rightarrow \sqrt{\rho} \in \mathbb{Z}$ *quindi* $\sqrt{\rho}$ *è un intero che divide* ρ *e* $1 < \sqrt{\rho} < \rho$ $\square$

Teorema 3 (Euclide)
Esistono infiniti numeri primi

Dimostrazione
Supponiamo per assurdo che $\exists$ *un numero finito di primi* $\rho_1, \dots, \rho_r$
Definiamo: $N := (\rho_1 \cdot \ldots \cdot \rho_r) + 1 > 1$
$\Rightarrow \exists \rho_k$ *primo tale che* $\rho_k | N$
$$\Rightarrow \begin{cases} \rho_k | N \\ \rho_k | N - 1 \end{cases} \Rightarrow \rho_k | N - (N-1) \Rightarrow \rho_k | 1, \text{ assurdo} \qquad \square$$

Definizione 3 (Numero di Euclide)
Sia ρ *primo*
$$\rho^{\#} := \left(\prod_{q \in \rho, q \ primo} q \right) + 1.$$
$\rho^{\#} + 1$ *si dice numero di Euclide*