Lezione 6 Algebra I

Federico De Sisti

2025-03-20

0.1 Esercizi Vari

Ricordo
Abbiamo dimostrato che $z \in \mathbb{Z}[i]$ tale che $\nu(z) = p$ con $p \in \mathbb{Z}$ primo
Allora primo in $\mathbb{Z}[i]$
Esercizio:
Se $p \in \mathbb{Z}$ è primo tale che $p \equiv_4 3$ dimostrare che p non è somma di due quadrati
Soluzione
In $\mathbb{Z}/(4)$ gli unici quadrati sono $[0]$ e $[1]$
Quindi se $p = a^2 + b^2 \Rightarrow a^2 + b^2 \equiv_4 p \equiv_4 3$ Assurdo poiché $3 \notin \{[0], [1]\}$
Esercizio:
Sia $p \in \mathbb{Z}$ primo $p \equiv_4 1$. Dimostrare che esiste $m \in \mathbb{Z}$ tale che $m^2 \equiv_p -1$
Soluzione Gauss:
Ricordo che esistono radici primitive in $\mathbb{Z}/(p)$
Sia r tale radice.
e sia $k = ind_r(-1) \quad (r^k \equiv_p (-1))$

$$r^{\frac{k(p-1)}{2}} \equiv_p (-1)^{\frac{p-1}{2}} \equiv_p 1$$

usando il fatto che $p \equiv_4 1$
Ricordo che $ord_{U_p}(r) = p - 1 \Rightarrow (p-1)|\frac{k(p-1)}{2} \Rightarrow \frac{k}{2}$
$\Rightarrow (r^{k/2})^2 \equiv_p r^k \equiv_p -1$
Soluzione Wilson:
$(p-1)! \equiv_p -1$
Ora $\phi \equiv_4 1 \;\Rightarrow\; p = 4n + 1, \quad n \in \mathbb{Z}_{>1}$
$\Rightarrow (4n)! \equiv_p -1$
$(4n)! = 1 \cdot 2 \cdot \ldots \cdot (2n) \cdot (2n+1) \cdot \ldots \cdot (4n)$
ma $2n + 1 \equiv_p -2n$ perché $p = 4n + 1_p 0 \Rightarrow 2n + 1 \equiv_p -2n$
quindi dopo la metà abbiamo gli stessi elementi che appaiono con segno inverso
Quindi $(4n)! \equiv_p (-1)^{2n} \cdot (2n)! \cdot (2n)! \equiv_p ((2n)!)^2$
Scelgo $m = (2n)!$

Proposizione 1
$p \in \mathbb{Z}$ primo. Allora p è primo in $\mathbb{Z}[i]$ se e solo se $p \equiv_4 3$

Dimostrazione
Studiamo vari casi

1. $p = 2 = (1+i)(1-i)$
   I due fattori $1 \pm i$ sono entrambi irriducibili perché $\nu(1 \pm i) = 2$ primo $\Rightarrow$ $1 \pm ip$ primo in Z[i]
   2 non è primo in $\mathbb{Z}[i]$

2. $p \in \mathbb{Z}$ *primo tale che* $p \equiv_4 3$
   Se p fosse riducibile in $\mathbb{Z}[i]$ allora $p = (a+ib)+(c+id)$ dove i due membri sono entrambi non invertibili.
   $p^2 = \nu(\phi) = \nu(a+ib)\nu(c+id) = (a^2+b^2)(c^2+d^2)$ *L'unica speranza per*

far si che venga p^2 è che entrambi i membri vengano p
$\Rightarrow Assurdopoiché p \equiv_4 3$

3. $p \equiv_4 1$, *Per l'esercizio esiste* $m \in \mathbb{Z}$ *tale che* $m^2 \equiv_p -1$
   $\Rightarrow p | m^2 + 1 = (m+i)(m-i)$
   Se per assurdo $p =$ *primo in* $\mathbb{Z}[i]$
   avremmo che $p|(m+i)$ *oppure* $p|(m-i)$
   $\Rightarrow$ *Assurdo perché* ϕ *non divide le parti immaginarie* $\Rightarrow p$ *non è primo in* $\mathbb{Z}[i]$

$\square$

Corollario 1 (Girard 1632, Fermat 1640, Eulero 1754)
$p \in \mathbb{Z}$ *primo dispari. Allora* p *è somma di due quadrati se e solo se* $p \equiv_4 1$

Dimostrazione
Abbiamo due casi

1. $p \equiv_4 3$ *già visto che* p *non è somma di due quadrati.*

2. $p \equiv_4 1$ *Sappiamo che* p *non è irriducibile in* $\mathbb{Z}[i]$
   $\Rightarrow p = w_1 \cdot w_2 \cdot \ldots \cdot w_k$
   con w_j *irriducibile in* $\mathbb{Z}[i]$ *e* $k \geq 2$
   $\Rightarrow p^2 = \nu(p) = \nu(w_1) \cdot \nu(w_2) \cdot \ldots \cdot \nu(w_k) \Rightarrow k = 2$ *dato che tutti i termini sono diversi da 1 (sono irriducibili)*
   $\nu(w_1) = \nu(w_2) = p \Rightarrow p = \nu(w_1) = a^2 + b^2$ *dove* $w_1 = a + ib$

$\square$

Corollario 2
$p \in \mathbb{Z}$ *primo tale che* $p \equiv_4 1$ *allora* $p = z \cdot \overline{z}$, *dove* $z \in \mathbb{Z}[i]$ *è primo.*

Dimostrazione
Dal corollario precedente abbiamo che $p = a^2 + b^2 = (a+ib)(a-ib)$ *devo controllare che lo* z *scelto* $(a+ib)$ *sia irriducibile*
$p^2 = \nu(p) = \nu(a+ib)\nu(a-ib)$ *e ogniuno di questi due termini ha effettivamente valutazione* p. $\square$

Esercizio
$z \in Z[i]$ è primo se e solo se $\overline{z} \in \mathbb{Z}[i]$ è primo.

Teorema 1
$z \in \mathbb{Z}[i]$ primo. Allora una delle seguenti condizioni è verificata:

1. $\nu(z) = p$ *con* $p \in \mathbb{Z}$ *primo tale che* $p \equiv_4 1$
2. $\nu(z) = p^2$ *con* $p \in \mathbb{Z}$ *primo tale che* $p \equiv_4 3$

Dimostrazione
Se $z \in \mathbb{Z}[i]$ *è primo* $\Rightarrow \nu(z) > 1$
$\Rightarrow \nu(z) = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ *con* $p_j \in \mathbb{Z}$ *primo.*
Studiamo vari casi

1. $p_1 = 2 \Rightarrow 2|v(z) \Rightarrow 2|z \cdot \overline{z} \Rightarrow 2|z$ *e* $2|\overline{z} \Rightarrow (1 \pm i)|z \Rightarrow$ *Assurdo perché* z *irriducibile*
2. $p_1 \equiv_4 3 \Rightarrow p_1$ *primo in* $\mathbb{Z}[i]$
   $\Rightarrow p_1|v(z) = z \cdot \overline{z} \Rightarrow p_1|z$ *oppure* $p_1|\overline{z}$ *quindi* p_1 *e* z *sono associati oppure* p_1 $\overline{z}$ *sono associati* ($\overline{z}$ *irriducibile)*
   $\Rightarrow p_1^2 = \nu(p_1) = \nu(z) = \nu(\overline{z})$ *da qui tesi*
3. $p_1 \equiv_4 1$
   $\Rightarrow p_1 = w \cdot \overline{w}$ *con* $w \in \mathbb{Z}[i]$ *primo*
   Allora $p_1|\nu(z) = z \cdot \overline{z}$
   $\Rightarrow w|z \cdot \overline{z}$
   $\Rightarrow w, z$ *associati oppure*
   $w, \overline{z}$ *associati*
   $\Rightarrow \nu(w) = \nu(z) = \nu(\overline{z})$

$\square$

Corollario 3
$a + ib \in \mathbb{Z}[i]$ è primo se e solo se vale una delle seguenti condizioni

1. $a = 0$ *se* $b \in \mathbb{Z}$ *sia primo tale che* $b \equiv_4 3$
2. $b = 0$ *se* $a \in \mathbb{Z}$ *sia primo tale che* $a \equiv_4 3$
3. $a \neq 0$, $b \neq 0$ $\;a^2 + b^2 \in \mathbb{Z}$ *è primo*

Dimostrazione
Se una delle condizioni vale allora $a + ib$ *è primo in* $\mathbb{Z}[i]$ *(l'ultima è vera per la valutazione).*
Viceversa: se $a + ib$ *è primo in* $\mathbb{Z}[i]$ *allora dal teorema segue che*

1. $\nu(a + ib) = pi \Rightarrow (3)$ *oppure* $\nu(a + ib) = p^2$ *con* $p \equiv_4 3$
   Nel secondo caso $a^2 + b^2 = p^2$
   $\Rightarrow p|\nu(a + ib)$
   $\Rightarrow p|(a + ib)(a - ib)$

$\Rightarrow p|(a+ib)$ *oppure* $p|(a+ib)$
$\Rightarrow p$ *associato ad* $a \pm ib$
$\Rightarrow p|a$ *e* $p|b$
$\Rightarrow \begin{cases} a = n_1 p \\ b = n_2 p \end{cases}$
$\Rightarrow p^2 = a^2 + b^2 = n_1^2 p^2 + n_2^2 p^2 - p^2(n_1^2 + n_2^2)$
$\Rightarrow \begin{cases} n_1 = \pm 1 \\ n_2 = 0 \end{cases} \quad oppure \quad \begin{cases} n_1 = 0 \\ n_2 = \pm 1 \end{cases}$ □
Esempi(Fattorizzazioni in $\mathbb{Z}[i]$)
fattorizzare in irriducibili, $25 \in \mathbb{Z}[i]$
$25 = 5 \cdot 5$
Quindi fattorizziamo $5 \in \mathbb{Z}[i]$
$5 = 4 + 1 = 2^2 + 1^2 = (2+i)(2-i)$
Ricorda
La fattorizzazione è unica a meno di moltiplicazioni per l'unità
$\Rightarrow 25 = (2+i)^2(2-i)^2$

fattorizza in irriducibili
$9 - 15i \in \mathbb{Z}[i]$
$9 - 15i = 3(3-5i)$
ma 3 è irriducibile in $Z[i]$
poiché $3 \equiv_4 3$
Basta fattorizzare $3 - 5i$
$\nu(3-5i) = 9 + 25 = 34 = 2 \cdot 17$
Assumiamo che
$(3-5i) = (1+i)(a+ib)$ con $v(a+ib) = 17$
$(1+i)(a+ib) = (a-b) + i(a+b) = 3 - 5i$
$\begin{cases} \text{a - b = 3} \\ \text{a - b = -5} \end{cases} \Rightarrow \begin{cases} \text{a = -1} \\ \text{b = -4} \end{cases}$
$\Rightarrow 9 - 15i = 3 \cdot (1+i) \cdot (-1-4i)$

Fattorizziamo $3 + 4i \in \mathbb{Z}[i]$
$\nu(3+4i) = 9 + 16 = 25 = 5^2$
$\Rightarrow 3 + 4i = (a+ib)(c+id)$
con $\nu(a+ib) = 5 = \nu(c+id)$
$\Rightarrow \begin{cases} ac - bd = 3 \\ bc + ad = 4 \end{cases}$
$\Rightarrow$ Per ottenere la prima uguaglianza abbiamo bisogno di $ac = 4$ e $bd = 1$, otteniamo poi $bc = 2$ e $ad = 2$
Scegliamo $a = c = 2$ $b = d = 1$
$\Rightarrow 3 + 4i = (2+i)^2$

Calcolare $MCD(3+4i, 4-3i)$ in $\mathbb{Z}[i]$
Osserviamo:

$-i(3+4i) = -3i - i^2 \cdot 3 = 4 - 3i$
Quindi:
$MCD = 3 + 4i$

0.2 Campo dei Quozienti

R dominio d'integrità.
L'obiettivo è definire un campo, $Frac(R)$, che contiene R come sottoanello, e soddisfa certe proprietà.
Tenendo in esempio $\mathbb{Q} = Frac(\mathbb{Z})$
Costruzione:
$X = \{(a, b) \mid a \in \mathbb{R}, b \in \mathbb{R} \setminus \{0\}\}$
definiamo la relazione di equivalenza
$(a, b) \sim (c, d) \Leftrightarrow ac = bd$ in R
Esercizio
Dimostra che questa è una relazione d'equivalenza su X
$Frac(R) = X/\sim$
si dice campo dei quozienti o delle frazioni di R con le operazioni $+$ e $\cdot$ definite da:

$$(a, b) \cdot (c, d) = (ac, bd) \in X.$$
$$(a, b) + (c, d) = (ad + bc, bd) \in X.$$

Esercizio
1) Le operazioni sono ben definite su $Frac(R)$
2) Verificare che $Frac(R)$ soddisfa la seguente proprietà universale:

$$\forall \text{ omomorfismo di anelli iniettivo } R \to K \text{ con } K \text{ campo.}$$