

Sappiamo che $p \in \mathbb{N}^{>0}$ è primo se:

1) $p > 1$

2) $ab = p \Rightarrow (a=1 \wedge b=p) \vee (a=p \wedge b=1)$

Proposizione (Proprietà Euclidea dei numeri primi):

$$p > 1 \text{ è primo} \Leftrightarrow p \mid ab \Rightarrow p \mid a \vee p \mid b$$

Dim.:

\Rightarrow : Sia p primo t.c. $p \mid ab \wedge p \nmid a$. Mostriamo che $p \mid b$:

$$\Rightarrow \text{MCD}\{a, p\} = 1 \Rightarrow 1 = ax + py \text{ con } x, y \in \mathbb{Z}$$

$$\Rightarrow b = (ab)x + (bx)p \text{ è multiplo di } p$$

\Leftarrow : $p \mid ab \Rightarrow p \mid a \vee p \mid b \Rightarrow$ supponiamo WLOG $p \mid a$:

$$a = px \Rightarrow p = pbx \Rightarrow bx = 1 \Rightarrow b = 1$$

q.e.d.

Def. (Elemento irriducibile / primo di un dominio):

Dati un dominio R , $a \in R \setminus \{0\}$ non invertibile, si dice che a è **IRRIDUCIBILE** se:

$$a = bc \Rightarrow b \text{ invertibile} \vee c \text{ invertibile}$$

Si dice che a è **PRIMO** se:

$$a \mid bc \Rightarrow a \mid b \vee a \mid c$$

Proposizione:

Ogni elemento primo è irriducibile.

Dim.:

$$a \text{ primo} \Rightarrow a = bc \text{ con } a \mid b \vee a \mid c$$

\Rightarrow se $a|b$ si ha $b = ax \Rightarrow a = ax$

$\Rightarrow a(cx - 1) = 0 \Rightarrow cx = 1 \Rightarrow c$ invertibile

q.e.d.

Esempio:

$$R = \mathbb{Z}[\sqrt{-5}] :$$

$\Rightarrow \mathcal{C}_{\sqrt{-5}} : \mathbb{Z}[\times] \rightarrow \mathbb{C} \Rightarrow \mathbb{Z}[\sqrt{-5}] = \text{Im } (\mathcal{C}_{\sqrt{-5}})$

$\Rightarrow \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ($\sqrt{-5}$ è radice di $x^2 + 5$)

$$\Rightarrow 9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

Mostriamo che $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ sono irriducibili.

$$\begin{aligned} \text{Definiamo } N(a + b\sqrt{-5}) &= (a + b\sqrt{-5})(a - b\sqrt{-5}) \\ &= \|a + b\sqrt{-5}\|^2 = a^2 + b^2 \end{aligned}$$

\Rightarrow si ha $N(rs) = N(r)N(s) \quad \forall r, s \in \mathbb{Z}[\sqrt{-5}]$

$$1) 3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

$$\begin{aligned} \Rightarrow N(3) = 9 &= N(a + b\sqrt{-5})N(c + d\sqrt{-5}) \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \end{aligned}$$

Possiamo supporre $a^2 + 5b^2 < c^2 + 5d^2$, allora:

$$a^2 + 5b^2 = 1 \vee a^2 + 5b^2 = 3$$

$$\Rightarrow a^2 + 5b^2 = 3 \quad \text{F}$$

$$\Rightarrow a^2 + 5b^2 = 1 \Rightarrow a = \pm 1 \Rightarrow b = 0$$

$\Rightarrow a + b\sqrt{-5}$ invertibile $\Rightarrow 3$ irriducibile

$$2) 2 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

$\Rightarrow 9 = (a^2 + 5b^2)(c^2 + 5d^2)$ e si procede come sopra

3) $2 - \sqrt{-5} \Rightarrow$ analogamente.

\Rightarrow i 3 elementi sono irriducibili, tuttavia NESSUNO è primo:

$$\Rightarrow 3 \mid (2+\sqrt{-5})(2-\sqrt{-5}) \wedge 3 \nmid (2+\sqrt{-5}) \wedge 3 \nmid (2-\sqrt{-5})$$

$\Rightarrow (2+\sqrt{-5})+3 \cdot 3 \wedge (2+\sqrt{-5})+3$ infatti:

$$3 = (2+\sqrt{-5})(a+b\sqrt{-5}) \Rightarrow 3 = (a^2 + 5b^2) 3$$

$$\Rightarrow a^2 + 5b^2 = 1 \Rightarrow a = \pm 1 \wedge b = 0 \quad \leftarrow$$

\Rightarrow ciò non avviene in $\mathbb{Z}[i]$

Proposizione (Esistenza della fattorizzazione in \mathbb{Z}):

Ogni intero $a > 1$ è prodotto di primi.

Dim.:

Per assurdo, sia m il minimo intero > 1 che non è prodotto di primi $\Rightarrow m$ non è primo $\Rightarrow m = ab$ con $a, b \neq 1$ positivi $\Rightarrow 1 < a, b < m \Rightarrow a, b$ sono prodotti di primi \leftarrow

q.e.d.

Proposizione (Unicità della fattorizzazione in \mathbb{N}):

Se a è un intero > 1 e $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ con p_i, q_i primi, allora $r = s \wedge p_i = q_i \quad \forall i = 1, \dots, r$

Dim.:

Induzione su r (supponiamo WLOG $p_r \geq q_s$):

$$r=1 \Rightarrow p_1 = q_1 q_2 \dots q_s \Rightarrow p_1 \mid q_s \Rightarrow p_1 = q_s$$

$$r-1 \rightsquigarrow r \Rightarrow p_r \geq q_s \Rightarrow p_r \mid a \Rightarrow p_r \mid q_s \text{ per un certo } s$$

$$\Rightarrow p_r \geq q_s \Rightarrow p_r = q_s \Rightarrow p_r = q_s$$

$$\Rightarrow p_1 \dots p_{r-1} = q_1 \dots q_{s-1} \Rightarrow r-1 = s-1 \Rightarrow p_i = q_i$$

q.e.d.

Sia $R = \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\} \Rightarrow R$ è sottoripaello di $\mathbb{Q}[x]$ \Rightarrow sia $x \in R$ con $x = \frac{1}{2}x$, allora $2x \in R$, inoltre:

$$\frac{1}{2}x = 2 \cdot \frac{1}{4}x, \quad \frac{1}{4}x = 2 \cdot \frac{1}{8}x, \dots$$

$\Rightarrow \exists$ elementi di R che non sono prodotto di irriducibili (x non è prodotto di irriducibili).

Def. (Dominio a Fattorizzazione Unica):

Si dice che un dominio R è a **FATTORIZZAZIONE UNICA (UFD)** se ogni elemento $a \in R \setminus \{0\}$ è prodotto di irriducibili e, se $a = b_1 \dots b_r = c_1 \dots c_s$, allora $r=s \wedge \exists T \in S_r$ t.c. ci sia associato a $b_{T(i)}$ per $i=1, \dots, r$

Teorema (Caratterizzazione degli UFD):

R è UFD se e solo se:

1) ogni irriducibile in R è primo

2) $\exists \{\alpha_i\} \subseteq R$ successione t.c. $\alpha_0 R \subsetneq \dots \subsetneq \alpha_i R$

Dim.:

(\Leftarrow): Supponiamo che valgano 1,2:

\Rightarrow se $\exists a \in R \setminus \{0\}$ non invertibile che non è

prodotto di irriducibili, allora a non è irriducibile.

$a = bc$ con b, c non invertibili.

\Rightarrow uno fra b e c non è prodotto di irriducibili.

$\Rightarrow a_0 = a, a_1 = b \vee a_1 = c \Rightarrow a_1 = b_1 c_1 \dots$

$\Rightarrow a_0 R \not\subseteq a_1 R \not\subseteq \dots$ dato che:

$$a_n = a_{n+1} c_{n+1} \text{ MA } a_{n+1} \notin a_n R$$

\Rightarrow poiché vale 2, questa è una contraddizione \square

Supponiamo $a = b_1 \dots b_r = c_1 \dots c_s$ con b_i, c_j irriducibili

\Rightarrow Induzione su r

$r=1 \Rightarrow b_1 = c_1 \dots c_s \Rightarrow s=1$ perché $b_1 | c_s$ per

$$\text{un certo } s \Rightarrow c_s = b_1 u \Rightarrow b_1 = b_1 \left(\frac{c_1 \dots c_s}{c_s} \right) u$$

Caso generale: $b_r | c_1 \dots c_s$ ($r > 1$) \Rightarrow con una

permutazione, supponiamo $b_r | c_s$

$$\Rightarrow c_s | bu \Rightarrow b_1 \dots b_{r-1} = (c_1 u) c_2 \dots c_{s-1}$$

$$\Rightarrow r-1 = s-1$$

\Rightarrow : Sia R un UFD, e sia $a \in R$ irriducibile.

se $a | bc$, allora $b = b_1 \dots b_r, c = c_1 \dots c_s$ prodotti di irriducibili $\Rightarrow bc = ad$ con $d = d_1 \dots d_t$ prodotto di irriducibili $\Rightarrow b_1 \dots b_r \cdot c_1 \dots c_s = ad_1 \dots d_t$ sono tutti irriducibili \Rightarrow per l'unicità, a è associato a b_s o a c_s . Ma allora $a | b$ val c. Verifichiamo no

②: sia $a_0 R \subseteq \dots \subseteq a_i R$, se $a_0 R = \{0\}$

ci spostiamo e prendiamo $a_0 R \neq \{0\}$

$\Rightarrow a_0$ NON è invertibile, la sua decomposizione in

fattori irriducibili ho r fattori. also e quindi la decomposizione di α_1 ha meno di r fattori. \hookrightarrow
q.e.d.

Lemma:

Se $I_0 \subseteq \dots \subseteq I_m \subseteq \dots$ sono ideali di R (con R anello qualsiasi), allora $\bigcup_{n>0} I_n$ è un ideale

Def. (Ideale Primo):

Un ideale P di un anello commutativo R si dice **PRIMO** se si ha:

$$ab \in P \Rightarrow a \in P \vee b \in P \quad \forall a, b \in R$$

Proposizione:

Dato un dominio R , si ha:

$$a \in R \text{ è primo} \Leftrightarrow aR \text{ è ideale primo}$$

Proposizione:

Se I è un ideale di un anello commutativo R , si ha:

$$I \text{ è ideale primo} \Leftrightarrow R/I \text{ è dominio}$$

Dim.:

Osserviamo che $(a+I)(b+I) = 0+I \Leftrightarrow ab \in I$

q.e.d.

Corollario:

Ogni ideale massimale di un anello commutativo è primo

Dim.:

Ogni campo è un dominio

q.e.d.

Quando è possibile dire che aR è primo? (R commutativo)

\Rightarrow se $a=0$, ciò avviene quando R è un dominio

\Rightarrow se $a \neq 0$ non invertibile e R è PID, aR deve essere massimale

Teorema:

Ogni PID è un UFD

Dim.:

1) $a \neq 0$ non invertibile \Rightarrow se a è irriducibile, allora a è primo perché aR è massimale, quindi aR è primo.

2) $a_0R \subseteq \dots \subseteq a_nR \Rightarrow \bigcup_m a_m R = bR$ per un certo $b \in R$ $\Rightarrow b \in a_n R$ per un certo $n \Rightarrow bR \subseteq a_n R \subseteq \dots \subseteq bR \Rightarrow a_m R = a_n R \quad \forall n > m$

q.e.d.

Teorema:

Se R è UFD, allora $R[x]$ è UFD. In particolare, se F è un campo, $F[x]$ e $F[x][y] = F[x,y]$ sono UFD

