A proposito del polinomio razionale X^4+1

1. La irriducibilità in $\mathbb{Q}[X]$.

Se $a, b \in \mathbb{R}$ sono tali che

$$\begin{cases} a^2 - b^2 &= 0 \\ 2ab &= 1 \end{cases}$$

allora

$(a+ib)^2 = i,$

ossia il numero complesso

$z = a + ib$

è una radice quadrata di i,

e quindi una radice quarta di -1,

ossia, ancora, una radice del polinomio $f(X) = X^4 + 1$.

Un numero siffatto è

$$z = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i.$$

Ma insieme a z sono radici dello stesso polinomio $f(X)$ anche

- il suo complesso coniugato $\overline{z} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$ ($f(X)$ è a coefficienti reali);
- il suo opposto $-z = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$ ($f(X)$ è pari);
- il complesso coniugato del suo opposto $-\overline{z} = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i.$

Quindi in $\mathbb{C}[X]$ il polinomio $f(X)$ si decompone nel modo seguente:

$f(X) = (X - z)(X - \overline{z})(X + z)(X + \overline{z}).$

Se ne ricava la seguente decomposizione in $\mathbb{R}[X]$:

$$f(X) = \left(X^2 - 2Re(z)X + ||z||\right)\left(X^2 + 2Re(z)X + ||z||\right) = \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right).$$

Se $f(X)$ fosse riducibile in $\mathbb{Q}[X]$, ossia se ammettesse in $\mathbb{Q}[X]$ una decomposizione non banale, allora, non possedendo $f(X)$ radici reali, questa dovrebbe essere necessariamente costituita da due polinomi di

$\mathbb{Q}[X]$ irriducibili (in $\mathbb{R}[X]$, a maggior ragione in $\mathbb{Q}[X]$) aventi grado 2. Questi, per il Lemma di Gauss, potrebbero essere scelti in modo da avere coefficienti interi. Il prodotto dei loro coefficienti direttori dovrebbe essere pari a 1, quindi, a meno di passaggio agli opposti, si potrebbe supporre che entrambi i polinomi siano monici. Ma allora questi, per l'unicità della fattorizzazione in $\mathbb{R}[X]$, dovrebbero coincidere con quelli della precedente decomposizione, che, però, non appartengono a $\mathbb{Q}[X]$.
Ciò prova che $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

2. La riducibilità modulo *p*

Sia ora p un primo positivo. Proviamo che la riduzione $\overline{f}(X)$ di $f(X)$ modulo p è riducibile in $\mathbb{Z}_p[X]$. Se esiste un elemento ω di $\mathbb{Z}_p$ tale che $\omega^2 = -1$, allora in $\mathbb{Z}_p[X]$ il polinomio $\overline{f}(X)$ ammette la seguente decomposizione:

$$\overline{f}(X) = \left(X^2 - \omega\right)\left(X^2 + \omega\right).$$

Supponiamo allora che non esista un elemento siffatto. In tal caso $p > 2$, e dunque p è dispari. Proviamo che esiste un elemento α in $\mathbb{Z}_p$ tale che $\alpha^2 \in \{[2]_p, -[2]_p\}$. Ciò consentirà di decomporre il polinomio $\overline{f}(X)$ come

$$\overline{f}(X) = \left(X^2 + \alpha X + [1]_p\right)\left(X^2 - \alpha X + [1]_p\right)$$

oppure

$$\overline{f}(X) = \left(X^2 + \alpha X - [1]_p\right)\left(X^2 - \alpha X - [1]_p\right)$$

Basterà provare che l'insieme $\mathbb{Z}_p^*$ è l'unione disgiunta dei seguenti due sottoinsiemi:

$$\left\{[a]_p^2 \mid 1 \le a \le \frac{p-1}{2}\right\} \qquad \text{e} \qquad \left\{-[a]_p^2 \mid 1 \le a \le \frac{p-1}{2}\right\}.$$

Infatti, allora potremo dedurre che $[2]_p$ si trova in uno di essi. Ora, dati due distinti interi a_1, a_2 tali che $1 \le a_i \le \frac{p-1}{2}$, non può essere $[a_1]_p^2 = [a_2]_p^2$, poiché ciò implicherebbe

$\left([a_1]_p - [a_2]_p\right)\left([a_1]_p + [a_2]\right) = [0]_p$, ossia, data l'integrità di $\mathbb{Z}_p$, $\begin{cases} [a_1]_p = [a_2]_p, \\ \text{oppure} \\ [a_1]_p = -[a_2]_p \end{cases}$

ma entrambe le opzioni sono impossibili per ipotesi. Ciò prova che gli elementi del primo insieme sono a due a due distinti, e lo stesso vale per gli elementi del secondo insieme. Resta da provare che i due insiemi sono disgiunti. Ora, dati gli interi a_1, a_2 (non necessariamente distinti) tali che $1 \le a_i \le \frac{p-1}{2}$, se fosse $[a_1]_p^2 = -[a_2]_p^2$, allora, essendo $[a_2]_p^2$ invertibile (perché?), si avrebbe $\left([a_1]_p[a_2]_p^{-1}\right)^2 = [-1]_p$, contro la presente ipotesi. Ciò conclude la dimostrazione.