

1) Un polinomio $f(x) \in \mathbb{Q}[x]$ si dice primitivo, se i suoi coefficienti sono in $\mathbb{Z}$ e x il m.c.d. dei coefficienti vale 1.

Supponiamo $f \cdot g$ non primitivo. Allora esiste p primo t.c. p divide il m.c.d. dei coefficienti di $f \cdot g$.

Consideriamo l'app. $\varphi: \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ tale che

$$\varphi(a) = [a]_p \quad \forall a \in \mathbb{Z}$$

$$\varphi(x) = x$$

(φ estende con il teorema di estensione).

$$\text{Allora } \varphi(f \cdot g) = 0 \quad \text{Inoltre } \varphi(f \cdot g) = \varphi(f) \cdot \varphi(g),$$

quindi

$$\varphi(f) \cdot \varphi(g) = 0.$$

Essendo $\mathbb{Z}_p[x]$ un dominio d'integrità (anzi, campo),

$$\varphi(f) = 0 \quad \text{ o } \quad \varphi(g) = 0.$$

Quindi o tutti i coefficienti di f o tutti i coefficienti di g sono divisibili per p , quindi f o g non è primitivo.

2) Certamente $(x-2, y+3) \in \ker f$.

Se $F(x, y) \in \ker f$, consideriamo $F(x, y)$ come polinomio in y a coefficienti in $\mathbb{Q}[x]$ e dividiamolo per $y+3$.

Sì, allora $F(x, y) = (y+3) \cdot G(x, y) + R(x, y)$

dove $\deg_y R(x, y) < 1$, quindi R è un polinomio $R(x)$

nella sola x . Dividiamolo per $x-2$:

$$R(x) = H(x)(x-2) + R_1$$

dove $R_1 \in \mathbb{Q}$ è una costante. Essendo $\varphi(F(x, y)) = 0$,

otteniamo $\varphi((y+3) \cdot G(x, y) + H(x)(x-2) + R_1) = 0$

da cui $R_1 = 0$. Quindi $F(x, y) \in (x-2, y+3)$.

Poiché f è invertibile, abbiamo che

$$\frac{\mathbb{Q}[x, y]}{(x-2, y+3)} \cong \mathbb{Q}$$

e quindi $(x-2, y+3)$ è un ideale massimale.

3) Sia A anello finito e supponiamo che $a \in A$ non sia divisore dello zero. L'insieme $\{a^n \mid n \in \mathbb{N}\}$ è finito, quindi esistono $m, n \in \mathbb{N}$ diversi (per esempio $m > n$) tali che

$$a^n = a^m$$

Quindi $a^n - a^m = 0$ cioè $a^n (1 - a^{m-n}) = 0$

Se come a non è divisore dello 0, otteniamo $1 - a^{m-n} = 0$

cioè $a^{m-n} = 1$. Se $m = n+1$, otteniamo $a = 1$, che

a invertibile, e $m > n+1$, otteniamo

$$a^{m-n} = a^{m-n-1} \cdot a = 1, \text{ da cui segue che } a \text{ \textit{e} invertibile.}$$

$\mathbb{Z}, \mathbb{Q}[x], \mathbb{Z}[x]$ sono tutti esempi utili.

4). Se $\alpha, \beta \in H$ $\alpha < \beta$ sono del tipo: $\frac{a}{b}, \frac{c}{d}$ con $a, b, c, d > 0$. Allora $\frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{ad}{bc} \in H \subset H$

H sottogruppo di G .

G non \textit{e} ciclico: se fosse il numero razionale $\frac{a}{b}$ fosse un generatore, allora ogni elemento di G , cio\`e ogni numero razionale non nullo sarebbe della forma  $\left(\frac{a}{b}\right)^n$  con  $n \in \mathbb{Z}$ . Ma se  $p$  \textit{e} un numero primo che non compare ne\`e tra i fattori di a , ne\`e tra i fattori di  $b$ , non pu\`o esistere $n \in \mathbb{Z}$ t. che $\left(\frac{a}{b}\right)^n = p$. Per lo stesso motivo H non \textit{e} ciclico.

Consideriamo l'omomorfismo di gruppi

$$\varphi: G \longrightarrow C_2$$

$$\varphi\left(\frac{a}{b}\right) = \text{sgn}\left(\frac{a}{b}\right) = \begin{cases} 1 & \text{se } \frac{a}{b} > 0 \\ -1 & \text{se } \frac{a}{b} < 0 \end{cases}$$

$C_2 = \{-1, 1\}$ \textit{e} il gruppo ciclico di ordine 2.

q è normale e per $q = H$. Quando G/H è il gruppo ciclico di ordine 2.

5) Sia $[L : K] = n$ Quando sia $v_1, \dots, v_n$ una base di L come K -spazio vettoriale.

Pertanto gli elementi di L sono della forma

$$\lambda_1 v_1 + \dots + \lambda_n v_n \quad \text{con } \lambda_i \in K. \quad \underbrace{\quad}_{n \text{ volte}}$$

Se dunque K ha p^m elementi, L ha $\underbrace{p^m \cdot p^m \cdot \dots \cdot p^m}_n$ elementi, quando L ha $(p^m)^n = p^{mn}$ elementi.

Allora $p^n = p^{mn}$, da cui segue che $mn = n$, cioè che m divide n .