Algebra n. 3 - NOTE ALLA LEZIONE 22

Esempio 22.4

La dimostrazione lasciata per esercizio si trova alla pagina seguente.

Si ha:

$$P_1P_3 = (2, 1+i\sqrt{5})(3, 1+i\sqrt{5}) = (6)+(2+2i\sqrt{5})+(3+3i\sqrt{5})+(1+i\sqrt{5})^2 \subset (1+i\sqrt{5}),$$

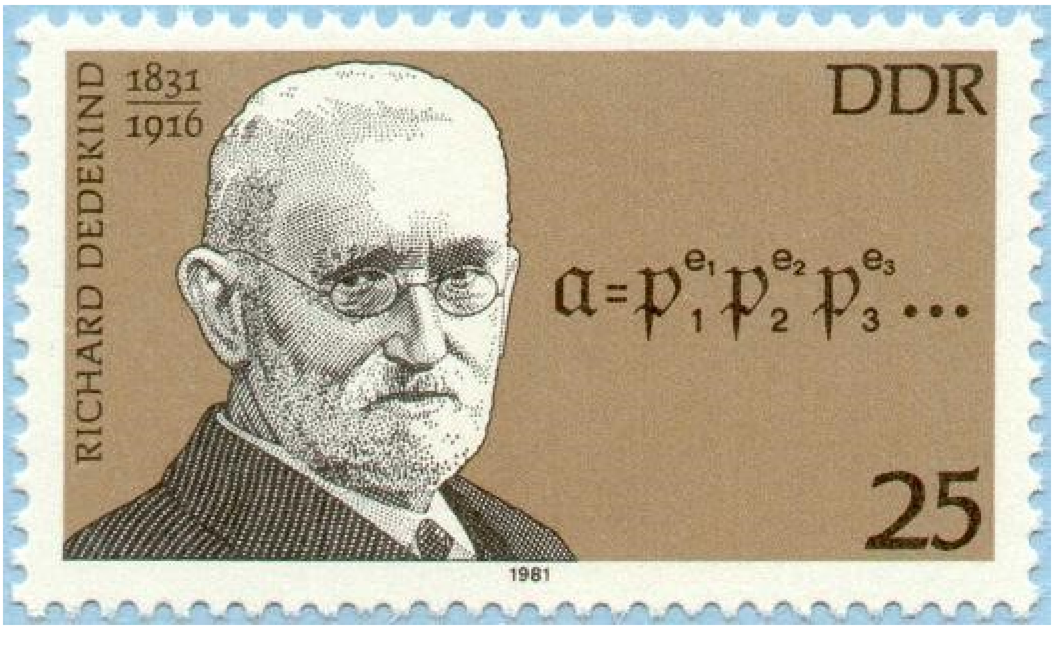
ma, d'altra parte, $1+i\sqrt{5} = 3+3i\sqrt{5}-(2+2i\sqrt{5}) \in P_1P_3$. Ciò prova che $(1+i\sqrt{5}) = P_1P_3$.

Esempio 22.7

Si ha $(2, 1+i\sqrt{5}) = (2, 1-i\sqrt{5})$, in quanto $1+i\sqrt{5} = -(-2+1-i\sqrt{5}) \in (2, 1-i\sqrt{5})$, e, d'altra parte, $1-i\sqrt{5} = 1+i\sqrt{5}-2i\sqrt{5} \in (2, 1+i\sqrt{5})$.

Proposizione 22.8

Nelle ipotesi della Proposizione, in virtù della Proposizione 19.20, si ha che $D_K = \mathbb{Z}[\sqrt{m}]$. Volendo applicare il Criterio di Kummer, essendo $f(x) = x^2 - m$ il polinomio minimo di $\sqrt{m}$ su $\mathbb{Q}$, occorre considerare la fattorizzazione della riduzione modulo p di $f(x)$ in $\mathbb{Z}_p[x]$. Questa è $\bar{f}(x) = (x-[a]_p)(x+[a]_p)$ nel caso a). Altrimenti $\bar{f}(x)$ è irriducibile, in quanto privo di radici in $\mathbb{Z}_p$. Dunque, nel caso a), in base al citato criterio, $(p) = (p, \sqrt{m}-a)(p, \sqrt{m}+a)$, altrimenti (p) è primo. [Nel caso a) si prendano $f_1(x) = x-a, f_2(x) = x+a$, altrimenti l'unico fattore primo dell'ideale (p) è $(p, f(\sqrt{m})) = (p)$.]



Dimostrazione che ${}^{\mathbb{Z}[i\sqrt{5}]}\!\big/_{P_1} \cong \mathbb{Z}_2$.

Si definisca l'applicazione $\varphi : \mathbb{Z}[i\sqrt{5}] \to \mathbb{Z}_2$ ponendo, per ogni $a,b \in \mathbb{Z}$, $\varphi(a+bi\sqrt{5}) = [a+b]_2$. Allora φ è un epimorfismo di anelli: poiché la surgettività e la conservazione della somma sono evidenti, basta osservare che, per ogni $a,b,c,d \in \mathbb{Z}$, il prodotto $(a+bi\sqrt{5})(c+di\sqrt{5}) = (ac-5bd)+(ad+bc)i\sqrt{5}$ viene inviato da φ nell'elemento $[ac+bd+ad+bc]_2 = [a+b]_2[c+d]_2$. Il nucleo di φ è costituito da tutti e soli gli elementi del tipo $a+bi\sqrt{5}$ con *a, b* interi entrambi pari o entrambi dispari. Tra questi figurano 2 e $1+i\sqrt{5}$ e, d'altra parte, ognuno di tali elementi è una combinazione lineare di questi ultimi a coefficienti in $\mathbb{Z}[i\sqrt{5}]$, poiché ammette una delle seguenti rappresentazioni:

$$2h+2ki\sqrt{5} \quad \text{oppure} \quad 2h+2ki\sqrt{5}+(1+i\sqrt{5}) \qquad \text{con } h,\, k \text{ interi.}$$

Ciò prova che il nucleo di φ è l'ideale $P_1 = (2, 1+i\sqrt{5})$. In base al Teorema fondamentale di omomorfismo per gli anelli, resta dunque indotto un isomorfismo tra ${}^{\mathbb{Z}[i\sqrt{5}]}\!\big/_{P_1}$ e $\mathbb{Z}_2$.