

Vilket svar är rätt?

R: röd, G: grön, B: blå

1. Om F är en kropp, $|F| = p^r$ (p primtal, $r \in \mathbb{Z}_+$),
finns då $a \in F$ med $a^2 + 1 = 0$?

R: ja, alltid G: bara ibland, B: nej, aldrig

2. Hur många olika generatorer har den multiplikativa
gruppen i kroppen $\mathbb{Z}_2[x]/(x^3 + x + 1)$?

R: 1 G: 4, B: 6

3. Vad är en partialbråksuppdelning av $\frac{x}{x^2+2} \in \mathbb{Z}_3[x]$?

R: $\frac{2}{x+1} - \frac{1}{x-1}$ G: $\frac{2}{x+1} + \frac{2}{x+2}$, B: $\frac{1}{x+1} + \frac{2}{(x+1)^2}$

4. Vad är karakteristiken för kroppen $\mathbb{Z}_5[x]/(x^3 + x + 4)$?

R: 5 G: 25, B: 125

Svar:

1. G, ty inte i $\mathbb{Z}_3$, men i $\mathbb{Z}_5$ (allmänt: omm $4 \mid (p^r - 1)$ eller $p = 2$).
2. B, ty $(\mathbb{Z}_2[x]/(x^3 + x + 1) \setminus \{0\}, \cdot)$ är en cyklisk grupp av ordning 7, så den har (eftersom 7 är ett primtal) 6 generatorer (alla element utom 1).
3. G (R), ty båda ger rätt resultat (men G har ”mer rätt” form (inga minustecken)).
Uppdelningen kan fås med handpåläggning eller, för att illustrera,
 $x^2 + 2 = (x + 1)(x + 2)$ och $1 = (x + 2) + 2(x + 1)$, så $x = x(x + 2) + 2x(x + 1) =$
 $= x(x + 2) + (2(x + 2) + 2)(x + 1) = (x + 2(x + 1))(x + 2) + 2(x + 1) = 2(x + 2) + 2(x + 1)$.
4. R, ty $1 + 1 + 1 + 1 + 1 = 0$, liksom i $\mathbb{Z}_5$.
Karakteristiken är alltid ett primtal, p om $|F| = p^r$.