

1. Costruire un campo con 9 elementi, scriverne gli elementi, e dimostrare che il gruppo moltiplicativo è ciclico.

Soluzione:

- i)*  $Z_3[x]/(x^2 + 1)$ ;
- ii)* polinomi di grado 0 e 1 su  $Z_3$ ;
- iii)*  $x + 1$  è un generatore.

2. Siano  $f, g \in Q[x]$ , e sia  $f$  irriducibile in  $Q[x]$ . Dimostrare che se  $f$  e  $g$  hanno una radice in comune  $\alpha$  (nel campo complesso), allora  $f$  divide  $g$ .

Soluzione: se  $f$  non divide  $g$ , allora essendo  $f$  irriducibile,  $f(x)h(x) + g(x)k(x) = 1$ . Calcolando in  $\alpha$ , si ha l'assurdo  $0 = 1$ .

3. Si consideri nell'anello  $Q[x]$  dei polinomi a coefficienti razionali l'insieme  $I$  dei polinomi  $f(x)$  che si annullano su  $\sqrt{2}$  e su  $\sqrt{3}$ . Dimostrare che:

- i)*  $I$  è un ideale di  $Q[x]$ ;
- ii)*  $I$  non è primo;
- iii)*  $I$  non è massimale;
- iv)* si determinino tutti gli ideali massimali contenenti  $I$

Soluzione: *i)* ovvio;

- ii)*  $(x - \sqrt{2})(x - \sqrt{3}) \in I$ , ma nessuno dei due polinomi sta in  $I$ ;
- iii)* un ideale massimale è primo;
- iv)* sono i due ideali generati da  $x^2 - 2$  e da  $x^2 - 3$ .

4. Sappiamo che nell'anello degli interi, ogni sottogruppo è un ideale. Dimostrare che questo fatto non è necessariamente vero nell'anello dei polinomi a coefficienti in un campo.

Soluzione: per ogni  $n \geq 0$ , i polinomi di grado  $\leq n$  formano un sottogruppo ma non un ideale.

5. Determinare i quozienti e i resti della divisione di  $3 - 2i$  per  $2 + i$  negli interi di Gauss.

Soluzione. Si ha

$$\frac{3-2i}{2+i} = \frac{4}{5} - \frac{7}{5}i$$

Il punto  $P = (4/5, -7/5) = (0.8, -1.4)$  si trova nel quadrato di vertici  $(0, -2), (0, -1), (1, -1), (1, -2)$ ;

*i)* distanza di  $(0, -2)$  da  $P$  è  $\sqrt{(4/5 - 0)^2 + (-7/5 + 2)^2} = 1$ ; quindi  $-2i$  non è un quoziente;

*ii)* la distanza di  $(0, -1)$  da  $P$  è  $\sim 0.89 < 1$ , e pertanto  $-i$  è un quoziente, con resto 2:  $3 - 2i = (2 + i) \cdot -i = 2$ ;

*iii)* la distanza di  $(1, -1)$  da  $P$  è  $\sim 0.45 < 1$ , e pertanto  $1 - i$  è un quoziente:  $3 - 2i = (2 + i) \cdot (1 - i) + (-i)$ ;

*iv)* la distanza di  $(1, -2)$  da  $P$  è  $\sim 0.63 < 1$ , e pertanto  $1 - 2i$  è un quoziente:  $3 - 2i = (2 + i) \cdot (1 - i) + (-1 + i)$ .