Cognome e Nome: _____
Matricola: _____
Data: _____

Algebra I

Risolvere coll'ausilio di GAP

1. Sia $F = \{a + \imath b\}$, ove $a, b \in \mathbb{F}_5$ e $\imath^2 = 2$, un campo con 25 elementi;.

   (a) determinare l'insieme $M = \{x \in F : x^5 = -x\}$;
   Siccome $(a+\imath b)^5 = a - \imath b$, $x = a + \imath b \in M$ sse $a = 0$ sse $x = \imath b \in \imath\mathbb{F}_5$.

   (b) detto G il gruppo moltiplicativo di F, provare che $f : M \times G \to M$, $f(m, g) = mg^6$, definisce un'azione di G su M;
   Poiché $|G| = 24$, g^6 appartiene all'unico sottogruppo di ordine $4 = \frac{24}{6}$ di G che a sua volta coincide col sottogruppo moltiplicativo di $\mathbb{F}_5$. Quindi $(g^6)^5 = g^6$ per ogni $g \in G$. Per cui $(mg^6)^5 = m^5 g^6 = -m(g^6) = -(mg^6)$ e $f(m, g) \in M$.
   La dimostrazione che f è un'azione è molto diretta. Ad esempio $m(gh)^6 = m(g^6 h^6) = (mg^6)h^6$.

   (c) determinare le orbite di questa azione.
   Se $m = 0$, allora l'orbita mG di m è $\{0\}$. Sia $m \neq 0$, allora $f(m, g) = m$ sse $mg^6 = m$ sse $g^6 = 1$. Quindi $C_G(m) = \{g \in G : g^6 = 1\}$. Siccome G è ciclico di ordine 24, $C_G(m)$ è l'unico sottogruppo di ordine 6 di G. Per cui $|mG| = |G : C_G(m)| = 4 = |M \setminus \{0\}|$, ossia l'orbita di m esaurisce tutti gli elementi non nulli di M. Quindi esistono 2 orbite $\{0\}$ e $\{\imath b : b \in \mathbb{F}_5, b \neq 0\}$.

2. Sia A una matrice 3×3 sui razionali, $V = \mathbb{Q}^3$ e $R = \mathbb{Q}[x]$ l'anello dei polinomi su $\mathbb{Q}$.

   (a) Dimostrare che $I = \{f \in \mathbb{Q}[x] : f(A) = 0\}$ è un ideale di $\mathbb{Q}[x]$ e provare quindi che I è principale (l'unico generatore monico di I viene detto il **polinomio minimo** di A e viene indicato con $m_A(x)$).
   Siano $f, g \in I$, $h \in R$, allora $(f + g)(A) = f(A) + g(A) = 0 + 0 = 0$ e $(h \cdot f)(A) = h(A)f(A) = h(A)0 = 0$. Quindi I è un ideale. Siccome R è un dominio a ideali principali $I = \langle m_A(x) \rangle$ per un unico polinomio monico $m_A(x)$.

   (b) Sia $m_A(x) = (x-1)(x-2)$. Usando l'identità di Bézout provare che
      i. $\ker(A - I_3) \cap \ker(A - 2I_3) = 0$;
      ii. $V = \ker(A - I_3) + \ker(A - 2I_3)$.

Sia $a(x) = x - 1$ e $b(x) = x - 2$. Allora a e b sono polinomi coprimi, quindi esistono $c, d \in R$ tali che $ac+bd = 1$. Si noti che $a(A) = A - I_3$ e $b(A) = A - 2I_3$. Sia $v \in V$, allora

$$v = vI_3 = va(A)c(A) + vb(A)d(A).$$

In particolare se

$$v \in \ker(A - I_3) \cap \ker(A - 2I_3),$$

allora

$$v = va(A)c(A) + vb(A)d(A) = 0c(A) + 0d(A) = 0.$$

Si osservi che per ogni $v \in V$, $va(A)c(A) \in \ker b(A)$. Infatti

$$va(A)c(A)b(A) = va(A)b(A)c(A) = vm_A(A)c(A) = v0c(A) = 0.$$

Analogamente $vb(A)d(A) \in \ker a(A)$, per cui

$$V = \ker(A - I_3) + \ker(A - 2I_3).$$

3. Sia $f(y) = y^4 - y^3 + 3y^2 + 2y - 1 \in \mathbb{Q}[y]$.

   (a) Mostrare che se $f(z) = 0$, $z \in \mathbb{C}$, allora $|z| < 4$.
   Basta applicare il teorema 4.42. Infatti, $a_0 = 1$ e $M = \max(|a_i|) = 3$. Per cui $|z| < 1 + \frac{3}{1} = 4$.

   (b) Provare che i fattori di f hanno grado 2 o 4 e che i coefficienti dei fattori di grado 2 hanno valore assoluto al massimo 16.
   Basta osservare che f non ammette radici razionali. Infatti $f(\frac{p}{q}) = 0$ sse $p|1$ e $q|1$. Ma $f(\pm 1) \neq 0$.
   Per le osservazioni a pag. 142, i coefficienti di un fattore di grado 2 di f sono in valore assoluto minori di $B_1 = \max\{\binom{2}{k}B^k : k = 1, 2\}$, ove $B = 4$ per il punto precedente.

   (c) Fattorizzare f applicando l'algoritmo di Berlekamp e il sollevamento di Hensel col primo $p = 5$. Quanti sollevamenti sono necessari?
   Il numero di sollevamenti n deve soddisfare $p^n > 2B_1$, ossia $5^n > 32$, per cui $n \geq 3$. Quindi bastano 2 sollevamenti.
   Applicando il codice in GAP che si trova nel file HenselLifting.gap si ottiene che $g(x) = x^4 - x^3 + 3x^2 + 2x - 1 \in \mathbb{F}_5[x]$ ha i seguenti fattori:

$$x^2 + x + Z(5)^0, x^2 + Z(5)^3x - Z(5)^0$$

   Questi possono essere visti come polinomi a coefficienti interi "ridotti" (ossia interi compresi tra $-\frac{p-1}{2}$ e $\frac{p-1}{2}$):

$$y^2 + y + 1, y^2 - 2y - 1.$$

Dopo un primo sollevamento ottengo:

$$y^2 + 6y + 11, y^2 - 7y + 9$$

e al terzo e ultimo sollevamento ottengo:

$$y^2 + 6y + 11, y^2 - 7y + 34.$$

Siccome questi polinomi non dividono f e non ho altri modi di comporre fattori irriducibili modulo 5 tra loro, ne segue che f è irriducibile.