*Duração: 2h30m* 18/01/06

*O primeiro grupo de questões é de escolha múltipla; uma resposta certa terá a cotação máxima que lhe for atribuída e uma resposta errada perderá metade dessa cotação (desde que a nota do exame permaneça não negativa).*
*Nas outras questões justifique convenientemente as suas respostas e indique os principais cálculos.*

1. Em cada uma das alíneas seguintes indique o valor lógico das afirmações:
   (**V**: verdadeira; **F**: falsa) **V F**

   (a) A divisão de polinómios é sempre possível em $\mathbb{Z}_{16}[x]$.

   (b) Se $n \in \mathbb{N}$ é um número primo então $\langle n \rangle$ é um ideal maximal de $\mathbb{Z}$.

   (c) $\mathbb{Q}(u) = \mathbb{Q}(u^2 + u + 1)$, onde $u^2 + u - 6 = 0$.

   (d) Se $L$ é uma extensão finita de $K$ e $[L : K]$ é um número primo, então $L$ é uma extensão simples de $K$.

   (e) O código (5,2)-linear binário definido pela matriz $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ corrige erros duplos.

2. Seja $A = (\mathbb{Q}, +, *)$, onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = 2ab$.

   (a) Mostre que $A$ é um anel comutativo com identidade.

   (b) Determine um subanel de $A$ que seja isomorfo ao anel usual $(\mathbb{Z}, +, \cdot)$ dos inteiros, descrevendo o isomorfismo (e justificando que é de facto um isomorfismo).

3. Determine:

   (a) O inverso de $\theta^2 - 6\theta + 8$ na extensão simples $\mathbb{Q}(\theta)$, onde $\theta$ satisfaz $\theta^3 - 6\theta^2 + 9\theta + 3 = 0$.

   (b) $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}]$ onde $\theta^2 + \sqrt{3}\theta + 3 = 0$.

   (c) O número de elementos do corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$.

4. Prove que:

   (a) Se $K$ é um corpo, o anel de polinómios $K[x]$ é de ideais principais.

   (b) Se $K$ não é um corpo, o anel de polinómios $K[x]$ não é necessariamente de ideais principais.

5. Mostre que:

   (a) O corpo $\mathbb{F}_{11}[x]/\langle x^2 + x + 4 \rangle$ é isomorfo a $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$.

   (b) A soma de todos os elementos de um corpo finito, com a excepção de $\mathbb{F}_2$, é 0.

---

1. **V F**

(a) A divisão euclidiana de polinómios é sempre possível em $\mathbb{Z}_{16}[x]$. [ ] [×]

`[Por exemplo, é impossível fazer a divisão pelo polinómio constante 2, uma vez que 2, sendo um divisor de zero de` $\mathbb{Z}_{16}$`, não é invertível.]`

(b) Se $n \in \mathbb{N}$ é um número primo então $\langle n\rangle$ é um ideal maximal de $\mathbb{Z}$. [×] [ ]

`[ O ideal` $\langle n\rangle$ `é maximal se e só se o anel quociente` $\mathbb{Z}/\langle n\rangle$ `é um corpo. Mas` $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$`, e` $\mathbb{Z}_n$ `é um corpo precisamente quando` $n$ `é primo, pelo que a afirmação é verdadeira.]`

(c) $\mathbb{Q}(u) = \mathbb{Q}(u^2+u+1)$, onde $u^2+u-6=0$. [×] [ ]

`[Como` $u^2+u=6$`, então` $\mathbb{Q}(u^2+u+1)=\mathbb{Q}(7)=\mathbb{Q}$`. Por outro lado, as duas raízes de` $x^2+x-6$ `são racionais (`$x=2$ `ou` $x=-3$`), pelo que também` $\mathbb{Q}(u)$ `coincide com` $\mathbb{Q}$`.]`

(d) Se $L$ é uma extensão finita de $K$ e $[L:K]$ é um número primo, então $L$ é uma extensão simples de $K$. [×] [ ]

`[Se` $L$ `é uma extensão finita de` $K$ `todos os seus elementos são algébricos sobre` $K$`. Como` $[L:K]=p>1$`, existe` $\theta\in L\setminus K$`. Pelo Teorema da Torre,` $p=[L:K]=[L:K(\theta)][K(\theta):K]$`. Como` $\theta\notin K$`,` $[K(\theta):K]>1$`. Mas` $p$ `é primo, donde só pode ser` $[K(\theta):K]=p$ `e` $[L:K(\theta)]=1$`. Esta última igualdade diz-nos que` $L=K(\theta)$`, pelo que` $L$ `é uma extensão simples de` $K$`.]`

(e) O código (5,2)-linear binário definido pela matriz $\begin{bmatrix} 1 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\end{bmatrix}$ detecta e corrige erros duplos. [ ] [×]

`[As palavras deste código são da forma` $(x_5, x_4+x_5, x_4+x_5, x_4, x_5)$ `com` $x_4,x_5\in\mathbb{Z}_2$`. O código é pois formado por 4 mensagens:` $(0,0,0,0,0)$`,` $(0,1,1,1,0)$`,` $(1,1,1,0,1)$`,` $(1,0,0,1,1)$`. Logo a sua distância mínima é 3. Portanto, detecta erros duplos mas só corrige erros singulares.]`

2. (a) Uma vez que $+$ é a adição usual, o par $(\mathbb{Q},+)$ é um grupo comutativo. Bastará então verificar que a operação $*$ é associativa, distributiva relativamente à adição e tem elemento neutro:

<u>Associatividade</u>: Para quaisquer $a,b,c\in\mathbb{Q}$ temos $a*(b*c)=a*(2bc)=2a2bc=4abc$ enquanto $(a*b)*c=(2ab)*c=4abc$, pelo que se confirma a propriedade.

<u>Distributividade</u>: Como $*$ é comutativa basta verificar uma das condições de distributividade: para quaisquer $a,b,c\in\mathbb{Q}$, $a*(b+c)=2a(b+c)=2ab+2ac=(a*b)+(a*c)$.

<u>Elemento neutro</u>: $1/2$ é elemento neutro de $*$ pois, para qualquer $a\in\mathbb{Q}$, $a*(1/2)=a$.

(b) Consideremos $S = \{a/2 : a \in \mathbb{Z}\} \subseteq \mathbb{Q}$, que é claramente um subanel de $A$: é não vazio e, para quaisquer $x = a/2, y = b/2 \in S$, tem-se $x - y = (a/2) - (b/2) = (a-b)/2 \in S$ e $x * y = 2xy = 2(a/2)(b/2) = ab/2 \in S$.

Também não é difícil ver que $(S, +, *) \cong (\mathbb{Z}, +, \cdot)$:

Como, para cada $x \in S$, $2x \in \mathbb{Z}$, podemos definir a função

$$\begin{array}{rccc} f: & (S,+,*) & \to & (\mathbb{Z},+,\cdot) \\ & x & \mapsto & 2x. \end{array}$$

É um homomorfismo de anéis: para quaisquer $x, y \in S$ tem-se $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$ e $f(x * y) = f(2xy) = 4xy = 2x2y = f(x)f(y)$.

É injectiva: $f(x) = f(y) \Leftrightarrow 2x = 2y \Leftrightarrow x = y$.

É sobrejectiva: para cada $a \in \mathbb{Z}$ seja $x = a/2 \in S$; evidentemente $f(x) = 2(a/2) = a$.

3. (a) O polinómio $x^3 - 6x^2 + 9x + 3$, do qual $\theta$ é raiz, é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$), logo é o polinómio mínimo $m(x)$ de $\theta$ sobre $\mathbb{Q}$. Seja $f(x) = x^2 - 6x + 8$. Uma vez que $m(x) = xf(x) + x + 3$ e $f(x) = (x-9)(x+3) + 35$ (o que confirma que $mdc(m(x), f(x)) = 1$), então

$$35 = f(x) - (x-9)(m(x) - xf(x)) = (x^2 - 9x + 1)f(x) - (x-9)m(x),$$

ou seja,

$$1 = \frac{1}{35}[(x^2 - 9x + 1)f(x) - (x-9)m(x)].$$

Substituindo $x$ por $\theta$ obtemos $1 = \frac{1}{35}(\theta^2 - 9\theta + 1)f(\theta)$, o que mostra que

$$(\theta^2 - 6\theta + 8)^{-1} = f(\theta)^{-1} = \frac{1}{35}(\theta^2 - 9\theta + 1).$$

(b) Pelo Teorema da Torre,

$$[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

Como $x^2 - 3$ é irredutível sobre $\mathbb{Q}$ (pelo critério de Eisenstein, $p = 3$), trata-se do polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$, donde $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Por outro lado, $\theta$ é raiz do polinómio $x^2 + \sqrt{3}x + 3 \in \mathbb{Q}(\sqrt{3})[x]$. Será este polinómio irredutível sobre $\mathbb{Q}(\sqrt{3})$? Pela fórmula resolvente das equações do segundo grau, as suas duas raízes são $\frac{-\sqrt{3} \pm \sqrt{3-12}}{2} \in \mathbb{C} \setminus \mathbb{R}$, ambas não reais. Logo, pelo critério das raízes, $x^2 + \sqrt{3}x + 3$ é irredutível sobre $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, donde $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}(\sqrt{3})] = 2$. Em conclusão, $[\mathbb{Q}(\sqrt{3}, \theta) : \mathbb{Q}] = 2 \times 2 = 4$.

(c) Uma vez que

$$\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle = \{p(x) + \langle x^2 + 1 \rangle \mid gr(p(x)) \leq 1\}$$

e existem precisamente $11 \times 11 = 121$ polinómios de grau menor que 2 em $\mathbb{F}_{11}[x]$, o corpo $\mathbb{F}_{11}[x]/\langle x^2 + 1 \rangle$ tem 121 elementos.

4. (a) Teorema 2.7 nos Apontamentos:

Seja $I$ um ideal de $K[x]$. Se $I = \{0\}$, então $I = \langle 0 \rangle$, que é um ideal principal. Podemos pois admitir que $I \neq \{0\}$.

Consideremos então o conjunto $N = \{n \in \mathbb{N}_0 \mid \text{ existe } s(x) \in I, gr(s(x)) = n\}$. É claro que, como $I \neq \{0\}$, $N$ é não-vazio, pelo que tem um mínimo. Seja $m(x)$ um polinómio em $I$ de grau igual a esse mínimo (podemos supor que $m(x)$ é mónico; com efeito, se não fosse, isto é, se o coeficiente do termo de maior grau fosse igual a $a \neq 1$, poderíamos sempre considerar o polinómio $n(x) = a^{-1}m(x) \in I$).

Provemos que $I$ é principal mostrando que $I = \langle m(x) \rangle$. Como $m(x) \in I$, é óbvio que $\langle m(x) \rangle \subseteq I$. Por outro lado, se $p(x) \in I$, usando o algoritmo de divisão temos $p(x) = q(x)m(x) + r(x)$, onde $gr(r(x)) < gr(m(x))$. Dado que $I$ é um ideal, podemos concluir que $r(x) = p(x) - q(x)m(x) \in I$. Mas então $r(x)$ só pode ser igual a 0 pois, com excepção do polinómio nulo, não pode haver nenhum polinómio em $I$ de grau inferior a $gr(m(x))$. Assim, $p(x)$ é um múltiplo de $m(x)$ pelo que pertence ao ideal $\langle m(x) \rangle$.

(b) Por exemplo, para $K = \mathbb{Z}$, o ideal $\langle 2, x \rangle$ de $K[x]$ não é principal.

5. (a) Como vimos na alínea (c) de 3, o corpo $\mathbb{F}_{11}[x]/\langle x^2+1 \rangle$ tem 121 elementos. Mas o corpo $\mathbb{F}_{11}[x]/\langle x^2+x+4 \rangle$ também tem 121 elementos, logo são necessariamente isomorfos (a $\mathbb{F}_{121} = \mathbb{F}_{11^2}$), pelo Teorema de Moore (Corolário 4.3 dos Apontamentos).

   (b) Qualquer corpo finito tem sempre um número de elementos igual a uma potência $p^n$ de um primo $p$, e esse corpo é isomorfo a $\mathbb{F}_p[x]/\langle r(x) \rangle$ para qualquer polinómio $r(x)$ de grau $n$ irredutível sobre $\mathbb{F}_p$. Os seus elementos são então as classes laterais $p(x) + \langle r(x) \rangle$ definidas pelos polinómios $p(x)$ de grau inferior a $n$:

| Grau | | | | | | |
|---|---|---|---|---|---|---|
| 0: | $0$ | $1$ | $2$ | $\cdots$ | $p-2$ | $p-1$ |
| 1: | $x$ | $x+1$ | $x+2$ | $\cdots$ | $x+p-2$ | $x+p-1$ |
| | $2x$ | $2x+1$ | $2x+2$ | $\cdots$ | $2x+p-2$ | $2x+p-1$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| | $(p-2)x$ | $(p-2)x+1$ | $(p-2)x+2$ | $\cdots$ | $(p-2)x+p-2$ | $(p-2)x+p-1$ |
| | $(p-1)x$ | $(p-1)x+1$ | $(p-1)x+2$ | $\cdots$ | $(p-1)x+p-2$ | $(p-1)x+p-1$ |
| 2: | $x^2$ | $x^2+1$ | $x^2+2$ | $\cdots$ | $x^2+p-2$ | $x^2+p-1$ |
| | $x^2+x$ | $x^2+x+1$ | $x^2+x+2$ | $\cdots$ | $x^2+x+p-2$ | $x^2+x+p-1$ |
| | $x^2+2x$ | $x^2+2x+1$ | $x^2+2x+2$ | $\cdots$ | $x^2+2x+p-2$ | $x^2+2x+p-1$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| | $x^2+(p-2)x$ | $x^2+(p-2)x+1$ | $x^2+(p-2)x+2$ | $\cdots$ | $x^2+(p-2)x+p-2$ | $x^2+(p-2)x+p-1$ |
| | $x^2+(p-1)x$ | $x^2+(p-1)x+1$ | $x^2+(p-1)x+2$ | $\cdots$ | $x^2+(p-1)x+p-2$ | $x^2+(p-1)x+p-1$ |
| | $2x^2$ | $2x^2+1$ | $2x^2+2$ | $\cdots$ | $2x^2+p-2$ | $2x^2+p-1$ |
| | $2x^2+x$ | $2x^2+x+1$ | $2x^2+x+2$ | $\cdots$ | $2x^2+x+p-2$ | $2x^2+x+p-1$ |
| | $2x^2+2x$ | $2x^2+2x+1$ | $2x^2+2x+2$ | $\cdots$ | $2x^2+2x+p-2$ | $2x^2+2x+p-1$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| | $2x^2+(p-2)x$ | $2x^2+(p-2)x+1$ | $2x^2+(p-2)x+2$ | $\cdots$ | $2x^2+(p-2)x+p-2$ | $2x^2+(p-2)x+p-1$ |
| | $2x^2+(p-1)x$ | $2x^2+(p-1)x+1$ | $2x^2+(p-1)x+2$ | $\cdots$ | $2x^2+(p-1)x+p-2$ | $2x^2+(p-1)x+p-1$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ |
| n-1: | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |

Não vale a pena listar mais polinómios pois já dá para observar o seguinte:

Caso 1: $p > 2$: Neste caso $p$ é ímpar, logo a soma (em $\mathbb{F}_p[x]$) dos polinómios em cada linha é sempre igual a 0 pois, como $p$ é ímpar, $1 + 2 + \cdots + p - 2 + p - 1$ é igual a

$$(1 + p - 1) + (2 + p - 2) + \cdots + (\frac{p-1}{2} + \frac{p+1}{2}) = p + p + \cdots + p = 0.$$

Portanto, a soma das respectivas classes em $\mathbb{F}_p[x]/\langle r(x)\rangle$ dá também 0.

Caso 2: $p = 2$, $n > 1$: Neste caso a lista de polinómios reduz-se a

| Grau | | |
|---|---|---|
| 0: | $0$ | $1$ |
| 1: | $x$ | $x+1$ |
| 2: | $x^2$ | $x^2+1$ |
| | $x^2+x$ | $x^2+x+1$ |
| 3: | $\cdots$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| n-1: | $x^{n-1}$ | $x^{n-1}+1$ |
| | $x^{n-1}+x$ | $x^{n-1}+x+1$ |
| | $x^{n-1}+x^2$ | $x^{n-1}+x^2+1$ |
| | $\vdots$ | $\vdots$ |

Agora a soma em cada linha não é 0 mas sim 1. Mas, como o número total de linhas é par (pois o número de polinómios de grau $p^{n-1}$ é igual ao número de polinómios de grau menor que $n-1$), a soma total continua a dar 0. Portanto, a soma das respectivas classes em $\mathbb{F}_p[x]/\langle r(x)\rangle$ é também igual a 0.