Departamento de Matemática da F.C.T.U.C.

Corpos e Equações Algébricas – Teste 2

4/5/2010

Nome (completo): ______________________________

Nota: *Justifique resumidamente as suas respostas.*

(1) Seja L uma extensão de um corpo K e $\alpha \in L$.
  (a) O que significa dizer que α é algébrico sobre K?
  (b) Sabendo que α é algébrico sobre K, defina polinómio mínimo de α sobre K.

(2) (a) Mostre que $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$ é um corpo. Indique a característica e o número de elementos deste corpo. Construa as tabelas de $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$.
  (b) $\mathbb{Z}_2[x]/ < x^2 + 1 >$ é um corpo? Justifique.

(3) Verifique se os seguintes polinómios são irredutíveis sobre $\mathbb{Q}$:

$$p(x) = x^4 - 2x^2 - 3, \qquad q(x) = 2x^5 + 6x^3 + 9x + 15.$$

Em caso negativo, factorize-o em polinómios irredutíveis.

(4) (a) Determine
    (i) $\mathbb{Q}(\sqrt{3}, \alpha)$ para cada uma das raízes α de $p(x) = x^4 - 2x^2 - 3$.
    (ii) o inverso de $\alpha + 1$ em cada uma das extensões da alínea anterior.
  (b) Mostre que $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3} + i)$.

RESOLUÇÃO:

(1) (a) $\alpha \in L$ diz-se algébrico sobre K se existe um polinómio $p(x)$ não nulo em $K[x]$ que tem α como raiz, isto é, tal que $p(\alpha) = 0$.
  (b) Se α é algébrico sobre K, consideremos o ideal $I = \{p(x) \in K[x] : p(\alpha) = 0\}$. Como K é um corpo, I é um ideal principal de $K[x]$ e tem-se então $I =< m(x) >$, com $m(x)$ um polinómio mónico em $K[x]$. O polinómio $m(x)$ é precisamente o único polinómio mónico e irredutível em $K[x]$ que tem α como raiz. A este polinómio chamamos o polinómio mínimo de α sobre K.

(2) (a) Sabemos que sendo K um corpo, o anel quociente $\mathbb{K}[x]/I$, é um corpo se e só se I é um ideal maximal de $K[x]$. Como em $K[x]$ todo o ideal é principal, isto equivale a dizer que $I =< p(x) >$ com $p(x)$ um polinómio irredutível sobre K. $\mathbb{Z}_2 = \{0, 1\}$ um corpo. O polinómio $x^2 + x + 1$ tem grau 2 e não tem raízes em $\mathbb{Z}_2$, então ele é irrredutível sobre $\mathbb{Z}_2$. Podemos agora concluir que $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$ é um corpo.
Se $p(x) \in \mathbb{Z}_2[x]$, pelo algoritmo da divisão válido em $\mathbb{Z}_2[x]$, tem-se $p(x) = q(x)(x^2 + x + 1) + r(x)$ com $r(x) \in \mathbb{Z}_2[x]$ um polinómio de grau 0 ou 1. Ou seja, $p(x)+ < x^2+x+1 >= ax + b+ < x^2 + x + 1 >$, com $a, b \in \mathbb{Z}_2$, e $\mathbb{Z}_2[x]/ < x^2 + x + 1 >= \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. (Escrevemos $\overline{p(x)} = p(x)+ < x^2 + x + 1 >$). Este corpo tem quatro elementos e tem característica 2, pois $1 + 1 = 0$ e $1 \neq 0$.
As tabelas deste corpo são

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

.

(b) Como x^2+1 é redutível em $\mathbb{Z}_2[x]$, pois $x^2+1=(x+1)(x+1)$ com $x+1\in\mathbb{Z}_2[x]$, tem-se $\overline{0}=<x^2+1>=x^2+1+<x^2+1>=(x+1+<x^2+1>)(x+1+<x^2+1>)$. Logo $\mathbb{Z}_2[x]/<x^2+1>$ tem divisores de zero e consequentemente não é corpo.

(3) O polinómio $q(x)=2x^5+6x^3+9x+15$ é irredutível sobre $\mathbb{Q}$ pelo critério de Eisenstein. Usando este critério com o primo $p=3$, verificamos que $3|15,9,0,6,0$, $3\nmid 2$ e $3^2\nmid 15$.

Um polinómio em $K[x]$, com K corpo, diz-se redutível sobre K, se o pudermos escrever como o produto de dois polinómios em $K[x]$, não constantes, e de grau inferior.

O polinómio $p(x)=x^4-2x^2-3$ tem grau quatro. Para ele ser redutível sobre $\mathbb{Q}$ ter-se-á de escrever ou como (1) produto de um polinómio de grau 1 por um de grau 3, ou como (2) produto de dois polinómios de grau 2, em $\mathbb{Q}[x]$. Mas como ±1 e ±3 não são raizes de $p(x)$, concluímos que $p(x)$ não tem ra'izes racionais. Isto significa que $p(x)$ não se factoriza num produto de um polinómio de grau 1 por um de grau 3. Resta a possibilidade de escrever $p(x)=(x^2+bx+c)(x^2+b'x+c')$ onde $a,b,c,a',b',c'\in\mathbb{Z}$. Da igualdade de polinómios $x^4-2x^2-3=x^4+(b+b')x^3+(c+c'+bb')xr+(bc'+b'c)x+cc'$ somos conduzidos ao sistema

$$\begin{cases} b+b'=0 \\ c+c'+bb'=-2 \\ bc'+b'c=0 \\ cc'=-3 \end{cases}$$

$$\begin{cases} b'=-b \\ c+c'-b^2=-2 \\ bc'-bc=0 \Leftrightarrow b(c-c')=0 \Leftrightarrow b=0 \vee c=c' \\ cc'=-3 \end{cases}$$

Se $c=c'$ vem $c^2=-3$ o que é impossível porque $c\in\mathbb{Z}$. Se $b=0$ vem

$$\begin{cases} b'=b=0 \\ c+c'=-2 \\ cc'=-3 \end{cases}$$

Multiplicando a segunda igualadade por c vem

$$\begin{cases} b'=b=0 \\ c^2+c'c=-2c \Leftrightarrow c^2+2c-3=0 \Leftrightarrow c=1 \vee c=3 \\ cc'=-3 \end{cases}$$

Neste caso temos $x^4-2x^2-3=(x^2+c)(x^2+c')=(x^2+1)(x^2-3)$ com $x^2-3,\quad x^2+1\in\mathbb{Z}[x]$. Estes polinómios são de grau 2 e as suas raízes, respectivamente, $\pm\sqrt{3},\quad \pm i$ são não racionais. Portanto, $x^2-3,\quad x^2+1$ são irredutíveis sobre $\mathbb{Q}$, e $x^4-2x^2-3=(x^2+1)(x^2-3)$ é a factorização em factores irredutíveis sobre $\mathbb{Q}$.

(4) (a) O polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}$ é $x^2-3\in\mathbb{Z}[x]$ pois é mónico e irredutível sobre $\mathbb{Q}$ e tem $\sqrt{3}$ por raiz. Logo $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$ e $\{1,\sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ como espaço vectorial sobre $\mathbb{Q}$. Vem então

$$\mathbb{Q}(\sqrt{3},\sqrt{3})=\mathbb{Q}(\sqrt{3},-\sqrt{3})=\mathbb{Q}(\sqrt{3})=\{a+b\sqrt{3}:a,b\in\mathbb{Q}\}.$$

Pelo Teorema da Torre, vem

$$[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}]=[\mathbb{Q}(\sqrt{3})(i):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2[\mathbb{Q}(\sqrt{3})(i):\mathbb{Q}(\sqrt{3})].$$

O polinómio mínimo de i sobre $\mathbb{Q}(\sqrt{3})$ é x^2+1 porque é um polinómio em $\mathbb{Q}[x]\subseteq\mathbb{Q}(\sqrt{3})[x]$ de grau dois e não tem raízes neste corpo. Caso contrário, existiriam $a,b\in\mathbb{Q}$ tais que $i=a+b\sqrt{3}\in\mathbb{R}$ o que é absurdo.
Logo $[\mathbb{Q}(\sqrt{3})(i):\mathbb{Q}(\sqrt{3})]=2$ e $\{1,i\}$ é uma base de $\mathbb{Q}(\sqrt{3})(i)$ como espaço vectorial sobre $\mathbb{Q}(\sqrt{3})$. Vem então $[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}]=4$ sendo $\{1,\sqrt{3}\}\{1,i\}=\{1,\sqrt{3},i,i\sqrt{3}\}$ uma base de $\mathbb{Q}(\sqrt{3},i)$ como espaço vectorial sobre $\mathbb{Q}$. Donde

$$\mathbb{Q}(\sqrt{3},i)=\mathbb{Q}(\sqrt{3},-i)=\{a+b\sqrt{3}+ci+di\sqrt{3}:a,b,c,d\in\mathbb{Q}\}.$$

(b) $\frac{1}{\sqrt{3}+1} = \frac{1-\sqrt{3}}{1-3} = -1/2 + \sqrt{3}/2 \in \mathbb{Q}(\sqrt{3})$; $\frac{1}{-\sqrt{3}+1} = -1/2 - \sqrt{3}/2$; $1/i = -i$; $1/(-i) = i \in \mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt{3}, i)$.

(c) $\mathbb{Q}(\sqrt{3}+i) \subseteq \mathbb{Q}(\sqrt{3}, i)$ e $1/(\sqrt{3}+i) = \sqrt{3}/4 - i/4 \in \mathbb{Q}(\sqrt{3}+i)$. Logo, $\sqrt{3}-i \in \mathbb{Q}(\sqrt{3}+i)$ e portanto também $\sqrt{3}+i+\sqrt{3}-i = 2\sqrt{3}$ ou ainda $\sqrt{3} \in \mathbb{Q}(\sqrt{3}+i)$. Analogamente $\sqrt{3}+i-\sqrt{3} = i \in \mathbb{Q}(\sqrt{3}+i)$. Temos então $\sqrt{3}, i \in \mathbb{Q}(\sqrt{3}+i)$ o que implica $\mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt{3}+i)$. Das duas inclusões anteriores obtemos $\mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}, i)$.