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

Corpos e Equações Algébricas – Frequência

Duração: 2h (Sem consulta) 2/6/2010

Nome (completo): _____

_____

Nota: *Justifique resumidamente as suas respostas e indique os principais cálculos.*

(1) Diga, justificando, se as seguintes afirmações são verdadeiras ou falsas.
   (a) No anel $(\mathbb{Z}_{10}; \oplus_{10}, \otimes_{10})$ todo o elemento não nulo ou é invertível ou é divisor de zero.
   (b) O polinómio $p(x) = (x^2+2)(3x^{11} + 12x^9 + 2x^5 + 16x^2 + 18x + 6)$ tem uma raiz real λ e $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 11$.
   (c) O menor subanel de $\mathbb{Z}$ que contém $\{8, 14\}$ é $2\mathbb{Z}$.
   (d) $\sqrt[3]{2-\sqrt{2}}$ é construtível a partir dos racionais.
   (e) É possível, usando régua não graduada e compasso, quadrar o círculo.

(2) (a) Seja L uma extensão do corpo K. Defina grau da extensão de L sobre K. O que significa dizer que a extensão de L sobre K é finita?
   (b) Sejam K, L e M corpos tais que L é uma extensão finita de K, e M é uma extensão finita de L. Prove que $[M : K] = [M : L][L : K]$.

(3) (a) Determine uma extensão L do corpo $\mathbb{Z}_2$ onde o polinómio $x^3 + x + 1 \in \mathbb{Z}_2[x]$ tenha uma raiz.
   (b) Indique o número de elementos de L.
   (c) Escreva $x^3 + x + 1$ em $L[x]$ como o produto de um polinómio linear por um polinómio do segundo grau.

(4) Seja θ a raiz real positiva do polinómio $x^4 - 2$. Determine $Gal(\mathbb{Q}(\theta), \mathbb{Q})$ o grupo de Galois da extensão $\mathbb{Q}(\theta)$ de $\mathbb{Q}$. (Observe que $\mathbb{Q}(\theta) \subseteq \mathbb{R}$.)

(5) Mostre que o polinómio $p(x) = 2x^5 - 5x^4 + 5$ não é resolúvel por radicais, sabendo que $p(-1) = -2$, $p(0) = 5$, $p(2) = -11$ e $p(3) > 0$.

RESOLUÇÃO:

(1) (a) Verdadeira. Seja $a \in \{1, 2, \ldots, 9\}$. Se $mdc(a, 10) = 1$ então existem inteiros r e s tais que $ra + 10s = 1$. Isto significa que existe um inteiro r tal que $ra \equiv 1 (\mod 10)$, ou, dito de outro modo, existe $r' \in \{1, 2, \ldots, 9\}$ tal que $r' \otimes_{10} a = 1$. Os elementos invertíveis de $\mathbb{Z}_{10}$ são então $1, 3, 7, 9$. Por outro lado, se $mdc(a, 10) = d > 1$ então $d|a$ e $d|10$. Escreva-se $dd' = 10$ e $a = kd$ onde $k, d, d' \in \{1, 2, \ldots, 9\}$. Então $ad' = kdd' = 10k$, ou seja, $a \otimes_{10} d' = 0$ e a (portanto, d' também) é um divisor de zero. Os divisores de zero de $\mathbb{Z}_{10}$ são $2, 4, 5, 6, 8$, pois $2 \otimes_{10} 5 = 4 \otimes_{10} 5 = 6 \otimes_{10} 5 = 8 \otimes_{10} 5 = 0$.

   (b) Verdadeira. Seja S um subanel de $\mathbb{Z}$ que contém $\{8, 14\}$. Como S é fechado para a adição, se $a \in S$ e $m \in \mathbb{Z}$ então $am \in S$. (Recorde que $am = \underbrace{a + \cdots + a}_{m vezes}$ se $m \geq 0$, e $am = \underbrace{(-a) + \cdots + (-a)}_{m vezes}$ se $m < 0$.) Pela mesma razão o $mdc(8, 14) = 2$ está também em S porque existem números inteiros r e s tais que $2 = 8r + 14s$. Assim $\{8, 14\} \subseteq 2\mathbb{Z} \subseteq S$. Ou seja, qualquer subanel de $\mathbb{Z}$ que contenha 8 e 14 contém o subanel $2\mathbb{Z}$. Isto significa que $2\mathbb{Z}$ é o menor subanel (no sentido da inclusão) de $\mathbb{Z}$ que contém o conjunto $\{8, 14\}$.

   (c) Verdadeira. Como $\mathbb{C}$ é algebricamente fechado e $p(x)$ tem grau 13, as treze raízes deste polinómio, constituídas pelas raizes de $x^2 + 2$ e pelas raízes de $3x^{11} + 12x^9 + 2x^5 + 16x^2 + 18x + 6$ estão em $\mathbb{C}$ sendo as não reais em número par pois estas são duas a duas conjugadas. Assim existe pelo menos uma raiz real λ que é necessariamente raiz de

$3x^{11}+12x^9+2x^5+16x^2+18x+6$ porque x^2+2 não tem raízes reais. O polinómio mínimo de λ sobre os racionais é o polinómio mónico $1/3(3x^{11}+12x^9+2x^5+16x^2+18x+6)$ irredutível sobre os racionais. Note-se que $3x^{11}+12x^9+2x^5+16x^2+18x+6$ é irredutível sobre os racionais pelo critério de Eisenstein com $p=3$. Donde $[\mathbb{Q}(\lambda);\mathbb{Q}]=11$.

(d) Falsa. Ponha-se $x=\sqrt[3]{2-\sqrt{2}}$. Então $x^3=2-\sqrt{2}$, $(x^3-2)^2=2$ e $\sqrt[3]{2-\sqrt{2}}$ é raiz do polinómio x^6-4x^3+2. Este polinómio é o polinómio mínimo de $\sqrt[3]{2-\sqrt{2}}$ sobre $\mathbb{Q}$ porque ele é mónico e irredutível sobre os racionais pelo critério de Eisenstein com $p=2$. Logo $[\mathbb{Q}(\sqrt[3]{2-\sqrt{2}});\mathbb{Q}]=6$. Como 6 não é uma potência de base 2, o número real $\sqrt[3]{2-\sqrt{2}}$ não é construtível (com régua não graduada e compasso) a partir dos racionais.

(e) Falsa. Veja-se a demonstração do Corolário 3.11, estudado na aula, página 83 dos apontamentos seguidos no curso, versão 2009.

(2) (a) Todo o corpo L tem a estrutura de espaço vectorial sobre um qualquer seu subcorpo K, tomando para adição vectorial a própria adição no corpo L, e para multiplicação escalar a multiplicação no corpo L. O grau da extensão de L sobre K é a dimensão de L como espaço vectorial sobre K. A extensão de L sobre K diz-se finita se a dimensão de L como espaço vectorial sobre K for finita.

(b) Enunciado, no caso de extensões finitas, do Teorema da Torre estudado na aula. Veja-se demonstração do Teorema 3.2, página 62, dos apontamentos seguidos no curso, versão 2009.

(3) (a) O polinómio $p(x)=x^3+x+1$ é irredutível sobre $\mathbb{Z}_2$ porque não tem raízes em $\mathbb{Z}_2$. De facto $p(0)=1=p(1)\neq 0$ e se ele fosse redutível sobre $\mathbb{Z}_2$ teria de ter pelo menos uma raiz em $\mathbb{Z}_2$. O ideal $I=<x^3+x+1>$ é maximal em $\mathbb{Z}_2$ e portanto o anel quociente $K=\mathbb{Z}_2[x]/I=\{0+I,1+I,x+I,x^2+I,1+x+I,1+x^2+I,x+x^2+I,1+x+x^2+I\}$ é um corpo finito. Identificando o polinómio $p(x)=x^3+x+1$ com a sua cópia em $K[x]$, $x+I$ é uma raiz em K de $p(x)=x^3+x+1$. (De facto $p(x+I)=(x+I)^3+(x+I)+(1+I)=x^3+x+1+I=0+I$.)

(b) Da alínea anterior o corpo $K=\mathbb{Z}_2[x]/I=\{0+I,1+I,x+I,x^2+I,1+x+I,1+x^2+I,x+x^2+I,1+x+x^2+I\}$ tem 2^3 elementos.

(c) Pondo $\theta=x+I$ e sabendo que $\theta^3+\theta+1=0$, efectua-se a divisão em $K[x]$ do polinómio x^3+x+1 por $x-\theta$ e obtém-se $x^3+x+1=(x-\theta)(x^2+\theta x+\theta^2+1$.

(4) As únicas raízes reais de x^4-2 são $\theta=\sqrt[4]{2}$, real positiva, e $-\sqrt[4]{2}$. As outras duas são não reais $\pm\sqrt[4]{2}\,i$.

A raiz real θ tem polinómio mínimo x^4-2 sobre $\mathbb{Q}$. Qualquer $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\theta)$, $\psi:\mathbb{Q}(\theta)\longrightarrow\mathbb{Q}(\theta)$ mantém fixos os números racionais e transforma θ numa raiz do mesmo polinómio em $\mathbb{Q}(\theta)=\mathbb{Q}(\sqrt[4]{2})\subseteq\mathbb{R}$. As únicas raízes que estão em $\mathbb{Q}(\theta)$ são $\theta=\sqrt[4]{2}$ e $-\theta=-\sqrt[4]{2}$. Logo, necessariamente, $\psi(\theta)=\theta$ ou $\psi(\theta)=-\theta$. Ou seja, ψ é a identidade ou $\psi_{-\theta}(a+b\theta+c\theta^2+d\theta^3)=a-b\theta+c\theta^2-d\theta^3$. Então, $Gal(\mathbb{Q}(\theta),\mathbb{Q})=\{id,\psi_{-\theta}\}\simeq\mathbb{Z}_2$.

(5) O critério de Galois diz que, se K é um corpo de característica zero e $p(x)\in K[x]$, então $p(x)$ é resolúvel por radicais se e só se $Gal(p(x);K)$ for um grupo resolúvel.

Sejam $p\geq 5$ um número primo, e $p(x)\in\mathbb{Q}[x]$ um polinómio irredutível de grau p. Se $p(x)$ tem exactamente duas raízes complexas não reais, então $Gal(p(x);\mathbb{Q})$ é o grupo simétrico $\mathbb{S}_p$ e como este grupo não é resolúvel para $p\geq 5$, então, pelo critério de Galois, $p(x)$ não é resolúvel por radicais.

O polinómio $p(x)=2x^5-5x^4+5$ como função real é uma função contínua e diferenciável e sabendo que $p(-1)=-2$, $p(0)=5$, $p(2)=-11$ e $p(3)>0$, então $p(x)$ tem pelo menos três raízes reais. Por outro lado, a derivada $p'(x)=10x^4-20x^3$ tem apenas duas raízes reais distintas. Então, pelo teorema de Rolle, não pode haver mais do que três raízes reais. Temos então um polinómio de grau cinco em $\mathbb{Q}[x]$ irredutível (pelo critério de Eisenstein com $p=5$) com exactamente três raízes reais. Pelo resultado anteriormente enunciado o seu grupo de Galois é $\mathbb{S}_5$ que não é resoluvel. Pelo critério de Galois podemos concluir que $p(x)$ não é resolúvel por radicais.