ÁLGEBRA – VE2 – 06/11/2014
GABARITO

PROFESSOR MARCO

Exercício 1. Encontre o corpo de fatoração K sobre F de $f(x) \in F[x]$ e calcule o grau da extensão $[K : F]$ para:
(i) $f(x) = x^4 - 2$ e $F = \mathbb{Q}$.
(ii) $f(x) = x^8 - 1$ e $F = \mathbb{F}_5$.

Solução: (i) As raizes de $f(x)$ são $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-i\sqrt[4]{2}$. Logo $K = \mathbb{Q}(\sqrt[4]{2}, i)$. O polinómio x^2+1 é irredutivel sobre $\mathbb{Q}$ pois não possui raizes sobre $\mathbb{Q}$ e é de grau 2, logo $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Come $\sqrt[4]{2}$ é raiz de $x^4 - 2$, temos $min(\mathbb{Q}(i), \sqrt[4]{2})$ divide $x^4 - 2$ e então $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] \leq 8$. De outro lado, note que $\sqrt[4]{2} \notin \mathbb{Q}(i)$, senão $\sqrt[4]{2} = \alpha + \beta i$, para $\alpha, \beta \in \mathbb{Q}$, que leva a um absurdo considerando potencias dos dois membros da equação. Logo $\mathbb{Q}(\sqrt[4]{2}, i) \neq \mathbb{Q}(\sqrt[4]{2})$, e como $min(\mathbb{Q}, \sqrt[4]{2}) = x^4 - 2$ (por Eisenstein), portanto $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}), i) : \mathbb{Q}(\sqrt[4]{2}] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \geq 8$. Logo $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}), i) : \mathbb{Q}] = 8$.

(ii) Temos $x^8 - 1 = (x^4 + 1)(x^4 - 1) = (x^4 + 1)(x^2 + 1)(x - 1)(x + 1)$. Note que $x^2 + 1$ tem 2 como raiz sobre $\mathbb{F}_5$ logo $x^2 + 1 = (x + 2)(x + 3)$. Usando quanto provado, temos também $x^4 + 1 = (x^2 + 2)(x^2 + 3)$. Os polinómios $x^2 + 2$ e $x^2 + 3$ são irredutíveis sobre $\mathbb{F}_5$ pois não possuem raizes. Afinal obtemos

$$x^8 - 1 = (x^2 + 2)(x^2 + 3)(x + 2)(x + 3)(x - 1)(x + 1)$$

Para encontrar o corpo de fatoração de $x^8 - 1$ tome $K = \mathbb{F}_5[x]/(x^2 + 2)$. Sobre K o polinómio $x^2 + 2$ fatora pois $\alpha = x + (x^2 + 2)$ é sua raiz. Note que 2α é raiz de $x^2 + 3$ pois $(2\alpha)^2 + 3 = 4\alpha^2 + 3 = 4(-2) + 3 = -5 = 0$. Portanto K é o corpo de fatoração de $x^8 - 1$ sobre $\mathbb{F}_5$ e $[K : \mathbb{F}_5] = 2$.

Exercício 2. Calcule o grupo de Galois $Gal(K/F)$ e diga se K/F é de Galois ou normal nos seguintes casos:
(i) $K = \mathbb{Q}(\sqrt{2}, i)$ e $F = \mathbb{Q}$;
(ii) $K = \mathbb{F}_p(\sqrt[p]{t})$ e $F = \mathbb{F}_p(t)$, onde t é uma indeterminada.

Solução: (i) Temos que todo $\sigma \in Gal(K/F)$ é determinado por $\sigma(\sqrt{2})$ e $\sigma(i)$. Além disso, $\sigma(\sqrt{2})$ é raiz de $min(\mathbb{Q}, \sqrt{2}) = x^2 - 2$ e $\sigma(i)$ de $min(\mathbb{Q}, i) = x^2 + 1$, logo

$$\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\} \text{ e } \sigma(i) \in \{i, -i\}.$$

Uma $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, i)$ é $\{1, \sqrt{2}, i, \sqrt{2}i\}$. Temos quatro $\mathbb{Q}$-autormorfismos de $\mathbb{Q}(\sqrt{2}, i)$ dados por

$$\sigma_1 = id, \quad \sigma_2(a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i) = a_1 - a_2\sqrt{2} + a_3 i - a_4\sqrt{2}i$$

$$\sigma_3(a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i) = a_1 + a_2\sqrt{2} - a_3 i - a_4\sqrt{2}i$$

$$\sigma_4(a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i) = a_1 - a_2\sqrt{2} - a_3 i + a_4\sqrt{2}i$$

e $Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}) = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$. Note que $\sigma_2^2 = \sigma_3^2 = \sigma_4^2 = id$, logo

$$Gal(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Como $[(\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}] = 4$, logo a extensão é de Galois. Como $\mathbb{Q}(\sqrt{2},i)$ é o corpo de fatoração de $(x^2-2)(x^2+1)$, a extensão é tambem normal.

(ii) Seja $K = \mathbb{F}_p(\sqrt[p]{t})$ e $F = \mathbb{F}_p(t)$. Temos que todo $\sigma \in Gal(K/F)$ é determinado por $\sigma(\sqrt[p]{t})$ e $\sigma(\sqrt[p]{t})$ é raiz de $min(\mathbb{F}_p(t), \sqrt[p]{t})$. Note que $\sqrt[p]{t}$ é raiz de $x^p - t$, e temos $x^p - t = (x - \sqrt[p]{t})^p$, logo $\sigma(\sqrt[p]{t}) = \sqrt[p]{t}$. Segue que $Gal(K/F) = \{id\}$. Em particular K/F não é de Galois, pois $[K : F] > 1$. A extensão K/F é normal, pois K é o corpo de fatoração de $x^p - t$ sobre F.

Exercício 3. Sejam p e q naturais primos. Prove que o polinómio $f(x) = x^p + 3x + 6$ é irredutível sobre $\mathbb{Q}(\sqrt{q})$.

Solução: O caso $p = 2$ é facil, pois neste caso o polinómio x^2+3x+6 possui raizes não reais e portanto as raizes não estão em $\mathbb{Q}(\sqrt{q})$, logo o polinómio é irredutível sobre $\mathbb{Q}(\sqrt{q})$.

Suponha $p \neq 2$ e seja α uma raiz de $f(x)$. Considere $K := \mathbb{Q}(\sqrt{q})$ e $L := K(\alpha)$. Suponha que $f(x)$ não é irredutível sobre K. Logo $grau(min(K,\alpha)) < grau(f(x) = p$ e portanto $[L : K] < p$. De outro lado $[K : \mathbb{Q}] = 2$, pois $min(\mathbb{Q}, \sqrt{q}) = x^2 - q$. Segue que $[L : \mathbb{Q}] = 2 \cdot [L : K]$. Como $f(x)$ é irreduível sobre $\mathbb{Q}$ por Eisenstein, temos $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. Como $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, conlcuimos que p divide $2 \cdot [L : K]$, onde $[L : K] < p$, o que é absurdo pois $p \neq 2$.

Exercício 4. Seja F um corpo e seja K/F uma extensão. Mostre que as seguintes condições são equivalentes:

(i) K é fecho algébrico de F;

(ii) K é o corpo de fatoração do conjunto de todos os polinómios não constantes com coeficientes em F.

Solução: Suponha que K é fecho algébrico de F e seja S o conjunto de todos os polinómios não constantes em $F[x]$. Para $f \in S$ e para uma raiz α de $f(x)$ (em alguma extensão de F), temos que α é algébrico sobre F (logo sobre K) e então $K(\alpha)/K$ é algébrica. Como K é algebricamente fechado, temos que $K(\alpha) = K$, i.e. $\alpha \in K$. Provamos assim que $f(x)$ possui todas as raizes sobre K, i.e. todo $f(x) \in S$ fatora linearmente sobre K. Dado $\alpha \in K$, logo α é algébrico sobre F pois K/F é algébrica. Logo α é raiz de $min(F,\alpha) \in F[x]$. Portanto $K = F(X)$, onde X é o conjunto de todas as raizes dos polinómios de S e então K é corpo de fatoração de S sobre F.

Viceversa, suponha que K é o corpo de fatoração do conjunto de todos os polinómios não constantes com coeficientes em F. Claramente K/F é algébrica. Seja L/K uma extensão algébrica de K. Vamos provar que $L = K$, e que portanto K é algebricamente fechado. De fato, se $\alpha \in L$, logo α é algébrico sobre K, e como K/F é algébrica, obtemos que α é algébrico sobre F também. Segue que α é zero do polinómio $min(F,\alpha) \in F[x]$ e portanto $\alpha \in K$, pois $min(F,\alpha) \in F[x]$ fatora linearmente sobre K.

Exercício 5. Seja V um espaço vetorial sobre um corpo K. Usando o lema de Zorn mostre que V possui uma base.

Solução: Podemos supor $V \neq 0$. Sia S o conjunto dos conjuntos linearmente independentes de V, ordenado por inclusão. Claramente S é não vazio. Dada uma cadeia em S, digamos $B_1 \subset B_2 \subset B_3 \subset \cdots$, temos que $B := \cup_{i\geq 1} B_i$ está em S. De fato, um subconjunto de vetores $\{v_1, \ldots, v_n\} \subset B$ é tal que é contido em algum B_m e portanto $v_1, \ldots, v_n$ são linearmente independentes.

Pelo Lema de Zorn existe um elemento maximal M de S. Portanto M é um conjunto linearmente independente. Vamos provar que M é uma base. Se de fato M não gera tudo V, existe v que não é combinação linear dos vetores de M. Mas pela maximalidade de M temos que $M \cup \{v\}$ é linearmente dependente, logo obtemos

$$cv + \sum c_i v_i = 0$$

onde $c, c_i \in K$ e $v_i \in M$. Podemos assumir que $c \neq 0$, pois M é um conjunto linearmente independente. A equação acima com $c \neq 0$ fornece v como comb. linear dos $v_i \in M$, contradição.