Trabalho 2
Grupos e Corpos

Yuri Kosfeld

Junho 2025

Exercício (4.1.8)**.** *a) Poderiámos provar utilizando Eisenstein, mas vamos mostrar por um processo analogo a um exemplo dessa seção. Informalmente, sabemos que uma raiz de* $x^2 - 3$ *é* $\sqrt{3}$*, assim sabemos que o polinomio pode ser reescrito como* $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$*. Então se* $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$*, o polinomio é redutivel. Suponha então que* $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$*. Logo* $\exists a, b \in \mathbb{Q}$ *tais que* $\sqrt{3} = a + b\sqrt{2}$*.*

$$\begin{aligned}(\sqrt{3})^2 &= (a + b\sqrt{2})^2 \\ 3 &= a^2 + 2ab\sqrt{2} + 2b^2 \\ &= (a^2 + 2b^2) + (2ab)\sqrt{2}\end{aligned}$$

Assim temos, $a^2 + 2b^2 = 3$ *e* $2ab = 0$*. Como* $2ab = 0$*, então ou* $a = 0$ *ou* $b = 0$*.*

- *Se* $a = 0$*, então* $2b^2 = 3 \Rightarrow b = \sqrt{3/2}$ *e logo* $b \notin \mathbb{Q}$*, absurdo.*
- *O caso* $b = 0$ *é analago ao anterior, também chegando em um absurdo.*

Logo $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ *e assim o polinomio é irredutivel. b)*

$$x^4 - 10x^2 + 1 = (x^2 - 2x\sqrt{3} + 1)(x^2 + 2x\sqrt{3} + 1)$$

$(x^2 - 2x\sqrt{3} + 1), (x^2 + 2x\sqrt{3} + 1)$ *são redutiveis em* $\mathbb{Q}[x]$*.*

Exercício (4.2.8)**.** *Seja* $a = p_1 p_2 \dots p_k$ *em que cada* p_i *é um primo distinto. Vamos usar o Criterio de Eisenstein. Seja* p *qualquer* p_i *da decomposição de* a*. Temos então que* $p \nmid 1$*,* $p \mid a$ *pela hipotese sobre* a*, mas* $p^2 \nmid a$*, já que cada primo da decomposição de* a *é diferente. Logo* $x^n - a$ *é irredutivel.*

Exercício (4.3.4)**.** *a) Suponha que* G *é um subgrupo de* L *que contém* F*, ou seja,* $F \subset G \subset L$*. Pelo Teorema de Extensão de Torres temos que*

$$p = [L : F] = [L : G][G : F]$$

Mas como p *é primo, a unico possibilidade para esse produto é* p *e 1. Assim temos dois casos:*

- *Se* $[L : G] = p$ *e* $[G : F] = 1$*, então sabemos que* $G = F$*.*
- *Se* $[L : G] = 1$ *e* $[G : F] = p$*, então segue que* $L = G$*.*

O que queriamos. b) Seja $\alpha \in L \setminus F$ *e considere* $F(\alpha)$*. Sabemos que* $F \subset F(\alpha) \subset L$*. Como vimos do item anterior, temos duas possibilidades, ou* $F(\alpha) = F$ *ou* $F(\alpha) = L$*. Mas* $\alpha \notin F$*, portanto* $F(\alpha) \neq F$*. Logo* $F(\alpha) = L$*.*

Exercício (4.4.4)**.** *Seja $L|F$ uma extensão finita de grau n. Sabemos que se ela é finita então é algebrica. Tome então $\alpha \in L$ e considere $F(\alpha)$. Sabemos que qualquer coleção de n+1 elementos em $F(\alpha)$ é L.D., então temos que $1, \alpha, \ldots, \alpha^n$ são L.D.. Portanto existem $a_0, a_1, \ldots, a_n \in F$ tais que*

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

Seja então $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Note então que $p(x) \in F[x]$ e $p(\alpha) = 0$, o que queriamos.

Exercício (5.1.4)**.** *As raizes da unidade do polinomio $f(x) = x^6 - 1$ são dadas por*

$$x = e^{2\pi ik/6} \quad k = 0, 1, 2, 3, 4, 5$$

Então temos:

$$1,\ e^{i\pi/3},\ e^{2i\pi/3},\ -1,\ e^{4i\pi/3},\ e^{5i\pi/3}$$

Note que a primeira raiz complexa é:

$$e^{i\pi/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

O corpo de decomposição de $f(x)$ deve conter todos as raízes. As raizes 1 e -1 já estão em $\mathbb{Q}$, então precisamos de um corpo $\mathbb{Q}(\alpha)$ tal que possue todas as demais raizes complexas. Note que a primeira raiz complexa pode ser escrita com $i\sqrt{3}$. Além disso, as demais raizes complexas são geradas a partir da primeira, logo $1, i\sqrt{3}$ geram todas as raizes. Portanto o corpo de decomposição de f é $\mathbb{Q}(i\sqrt{3})$.

Exercício (5.2.4)**.** *$\overline{\mathbb{Q}} \,|\, \mathbb{Q}$ é uma extensão normal que não é finita. Seja $p(x) \in \mathbb{Q}[x]$ o polinomio minimal de $\alpha \in \overline{\mathbb{Q}}$. Como $\overline{\mathbb{Q}}$ é algebricamente fechado, o corpo de decomposição de p está contido em $\overline{\mathbb{Q}}$. Logo a extensão é normal. Para todo p primo, já vimos que $x^p - 2$ é irredutivel em $\mathbb{Q}$. Temos que $[\mathbb{Q}(x^p - 2) : \mathbb{Q}] = p$. Como temos infinitos primos e $\overline{\mathbb{Q}}$ contém todos os corpos de decomposição dos polinomios dessa forma, segue que o grau da extensão é infinita entre $\overline{\mathbb{Q}}$ e $\mathbb{Q}$. Portanto é normal mas não é finita.*

Exercício (5.3.14)**.** *Tome $\alpha \in K$ um algebrico sobre F. Como $K \subset L$, $\alpha \in L$ e portanto é algebrico sobre F. Sabemos que $L \,|\, F$ é separavel, então o polinomio $p_{\alpha \,|\, F}$ é separavel. Logo $K \,|\, F$ é separavel. Tome agora $\beta \in L$ algebrico sobre K. Queremos mostrar que o polinomio minimal de β em K é separavel. Como $L \,|\, F$ é algebrico, $K \,|\, F$ é algebrico. Logo β é algebrico sobre F, portanto $p_{\beta \,|\, F}$ é separavel. Como $p_{\beta \,|\, K}$ divide $p_{\beta \,|\, F}$ e este é separavel, então $p_{\beta \,|\, k}$ também deve ser separavel.*

Exercício (5.4.7)**.** *Seja $K = F(\alpha_1, \ldots, \alpha_{n-1})$. Como cada α_i é separavel então $K \,|\, F$ é separavel. Note também que temos $L\,|\,K\,|\,F$, e como $L\,|\,F$ é finito, $K\,|\,F$ é também finito. Portanto pelo Teorema do Elemento Primitivo, $\exists\theta \in K$ tal que $K = F(\theta)$. Então agora temos $L = K(\alpha_n) = F(\theta)(\alpha_n)$. $\theta \in K$ é separavel sobre F já que $K \,|\, F$ é separavel. Como a extensão $FF(\theta)(\alpha_n)$ é finita, então $\exists\alpha \in K$ tal que $L = F(\alpha)$.*

Exercício (6.1.6)**.** *Note que $\sqrt{6}$ e $\sqrt{10}$ geram $\sqrt{15}$, por:*

$$\frac{\sqrt{6}\sqrt{10}}{2} = \frac{\sqrt{60}}{2} = \frac{2\sqrt{15}}{2} = \sqrt{15}$$

Então $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$. Calculamos agora o grau da extensão: O polinomio minimal de $\sqrt{6}$ e $\sqrt{10}$ são $x^2 - 6$ e $x^2 - 10$. Então

$$[\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{10})][\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = 2 \times 2 = 4$$

Exercício (6.2.3)**.** *a) O grau do polinomio* $x^4 + x^3 + x^2 + x + 1$ *é 4, então* $[\mathbb{Q}(w) : \mathbb{Q}] = 4$*. O polinomio minimal de* $\sqrt[5]{2}$ *é* $x^5 - 2$*, com grau 5 então* $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$*. Como* $w \notin \mathbb{R}$ *então* $w \notin \mathbb{Q}(\sqrt[5]{2})$*, logo temos:*

$$[L : \mathbb{Q}] = [\mathbb{Q}(w, \sqrt[5]{2}) : \mathbb{Q}(w)][\mathbb{Q}(w) : \mathbb{Q}] = 5 \times 4 = 20$$

b) Todas as raizes de $x^5 - 2$ *são* $w\sqrt[5]{2}$ *com* $w = e^{2\pi i/5}$*. Então* $\mathbb{Q}(w, \sqrt[5]{2})$ *é o corpo de decomposição.*

Exercício (6.3.2)**.** *a) Os polinomios minimais de* i *e* $\sqrt{2}$ *são* $x^2 + 1$ *e* $x^2 - 2$*. Então o grau da extensão é 4, portanto* $|Gal(\mathbb{Q}(i, \sqrt{2})|\mathbb{Q})| = 4$*. As raizes de* $x^2 + 1$ *são i e -i. Já as raizes de* $x^2 - 2$ *são* $\sqrt{2}$ *e* $-\sqrt{2}$*. Entao* $\sigma(i) \in \{i, -i\}$ *e fixa* $\sqrt{2}$*. E também* $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$ *fixa i. Logo* $\sigma^2 = Id$*. Portanto temos o grupo de Klein,* V_4*. b) Já analisamos o caso para i. O polinomio minimal de* $\sqrt[4]{2}$ *é* $x^4 - 2$*. Logo o grau da extensão é 8 e portanto* $|Gal(\mathbb{Q}(i, \sqrt[4]{2})|\mathbb{Q})| = 8$*. Todas as raizes de* $x^4 - 2$ *são* $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$*. Analogo ao caso anterior temos* $\{(1\,2\,3\,4), (2\,4)\} = D_4$*.*