0. Exemplos e mais exemplos

1. **Corpo primo e característica.** Seja $\mathbb{F}$ um corpo. Temos homomorfismo de anéis $\mathbb{Z} \to \mathbb{F}$ que leva 1 em 1. Temos duas possibilidades:

(1) o homomorfismo é injetor. Neste caso, dizemos que $\mathbb{F}$ tem característica 0, e escrevemos $\operatorname{char}\mathbb{F} = 0$ ou $\operatorname{car}\mathbb{F} = 0$. Ainda, $\mathbb{F}$ contém um subanel isomorfo a $\mathbb{Z}$, e portanto, $\mathbb{F}$ contém o menor corpo contendo o $\mathbb{Z}$, que é o corpo dos racionais. Daí, $\mathbb{F}$ contém $\mathbb{Q}$.

(2) o homomorfismo possui um núcleo, gerado por $p\mathbb{Z}$, com $p > 0$. Neste caso, dizemos que $\mathbb{F}$ possui característica p, e escrevemos $\operatorname{char}\mathbb{F} = p$ ou $\operatorname{car}\mathbb{F} = p$. Além disso, nesta situação, $\mathbb{F}$ contém $\{0, 1, \ldots, p-1\} \cong \mathbb{F}_p$ (em que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ é o corpo com p elementos). Daí $\mathbb{F}$ contém uma cópia de $\mathbb{F}_p$.

Definição 0.1. Seja $\mathbb{F}$ um corpo. Seu corpo primo é o menor subcorpo contido em $\mathbb{F}$.

Pelo visto acima, o corpo primo de $\mathbb{F}$ é ou $\mathbb{Q}$, ou algum $\mathbb{F}_p$, dependendo de sua característica.

Observação.

(i) Se $\operatorname{char}\mathbb{F} = p > 0$, então p é primo.

(ii) Além disso, se temos $\mathbb{F} \subseteq \mathbb{E}$, com $\mathbb{E}$ corpo, então $\operatorname{char}\mathbb{F} = \operatorname{char}\mathbb{E}$.

2. **Exemplo: $\mathbb{Q}[i]$.** Denote por $\mathbb{Q}[i]$ o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e $i \in \mathbb{C}$. Temos que

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Tal conjunto é um corpo: $\mathbb{Q}[i]$ é um anel comutativo com unidade, e dado $a+bi \neq 0$, temos $a^2 + b^2 \neq 0$. Então

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Existem outras formas de provar que $\mathbb{Q}[i]$ é um corpo, sem explicitamente exibir o inverso de cada elemento.

Temos que $\mathbb{Q} \subseteq \mathbb{Q}[i]$, e ainda, $\mathbb{Q}[i]$ é um $\mathbb{Q}$-espaço vetorial. Temos

$$\dim_{\mathbb{Q}} \mathbb{Q}[i] = 2.$$

Denotaremos $\mathbb{Q}[i]/\mathbb{Q}$, e diremos que $\mathbb{Q}[i]$ é uma *extensão* de $\mathbb{Q}$. O *grau* da extensão é $[\mathbb{Q}[i] : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}[i]$.

Note que o elemento i satisfaz o polinômio $X^2+1 \in \mathbb{Q}[X]$. Tal polinômio satisfaz as seguintes propriedades:

(1) $X^2 + 1$ é mônico,

(2) $X^2 + 1$ é irredutível em $\mathbb{Q}[X]$.

Por isso, denominaremos $X^2 + 1$ como sendo o *polinômio minimal de i sobre* $\mathbb{Q}$. Note que $[\mathbb{Q}[i] : \mathbb{Q}] = \operatorname{gr}(X^2 + 1)$.

Agora, considere o mapa $\psi_i : \mathbb{Q}[X] \to \mathbb{C}$ tal que $\psi_i(X) = i$. Note que $(X^2+1) \subseteq \ker\psi_i$. Ainda, $\ker\psi_i \neq \mathbb{Q}[X]$ (pois $\psi_i \neq 0$), e (X^2+1) é um ideal maximal de $\mathbb{Q}[X]$ (pois $X^2 + 1$ é irredutível em $\mathbb{Q}[X]$). Então, segue que $\ker\psi_i = (X^2 + 1)$. Além diso, $\operatorname{Im}\psi_i = \mathbb{Q}[i]$. Segue que

$$\mathbb{Q}[X]/(X^2 + 1) \cong \mathbb{Q}[i].$$

A construção de $\mathbb{Q}[X]/(X^2+1)$ tem a vantagem de ser uma construção abstrata e depende somente do corpo base $\mathbb{Q}$. Para $\mathbb{Q}[i]$, precisou-se da existência de um corpo maior (no caso, os complexos $\mathbb{C}$) e do elemento $i \in \mathbb{C}$.

Agora, $-i$ também é raiz de X^2+1. Então, as mesmas considerações podem ser feitas para obtermos

$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[-i].$$

Entretanto, $\mathbb{Q}[i] = \mathbb{Q}[-i]$. Ou, vale também a seguinte propriedade: $\mathbb{Q}[i]$ contém TODAS as raízes de X^2+1, que são i e $-i$.

Agora, quem é $\mathrm{Aut}(\mathbb{Q}[i])$? Veremos que será mais interessante considerar os automorfismos de $\mathbb{Q}[i]$ que são $\mathbb{Q}$-lineares. Equivalentemente, queremos os automorfismos que fixam os valores de $\mathbb{Q}$. Formalmente, queremos:

$$\begin{aligned}\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q}) &= \{\psi \in \mathrm{Aut}(\mathbb{Q}[i]) \mid \psi \text{ é } \mathbb{Q}\text{-linear}\} \\ &= \{\psi \in \mathrm{Aut}(\mathbb{Q}[i]) \mid \psi(q) = q, \forall q \in \mathbb{Q}\}.\end{aligned}$$

No caso de $\mathbb{Q}[i]$, é redundante pedir que os automorfismos sejam $\mathbb{Q}$-linear. Isso porque um automorfismo de um corpo automaticamente fixa os elementos do seu corpo primo. Entretanto, tal restrição será fundamental nas construções que desenvolveremos no curso.

Para determinar $\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})$, vamos procurar as inclusões (ou seja, homomorfismos não-nulos) $\mathbb{Q}[i] \to \mathbb{C}$ que são $\mathbb{Q}$-lineares.

Sabemos que existe a inclusão identidade $\iota : \mathbb{Q}[i] \to \mathbb{C}$. Agora, se $\sigma \in \mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})$, então obtemos outra inclusão $\mathbb{Q}[i] \xrightarrow{\sigma} \mathbb{Q}[i] \xrightarrow{\sigma} \mathbb{C}$. Daí

$$|\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})| \leq (\text{numero de homomorfismos injetor } \mathbb{Q}[i] \to \mathbb{C}).$$

Como $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$, vamos estudar os homomorfismos

$$\mathbb{Q}[X]/(X^2+1) \to \mathbb{C}.$$

Então, sejam $\psi : \mathbb{Q}[X]/(X^2+1) \to \mathbb{C}$ não nulo e $x = X + (X^2+1) \in \mathbb{Q}[X]/(X^2+1)$. Daí

$$0 = \psi(x^2+1) = (\psi(x))^2 + 1,$$

portanto, $\psi(x)$ é raiz de X^2+1. Segue que $\psi(x) \in \{i, -i\}$. Então, temos no máximo dois homomorfismos $\mathbb{Q}[X]/(X^2+1) \to \mathbb{C}$, e é elementar verificar que ambas estão bem definidas. Os conjuntos imagens são:

$$\begin{aligned}\mathbb{Q}[X]/(X^2+1) &\cong \mathbb{Q}[i] \subseteq \mathbb{C}, \\ \mathbb{Q}[X]/(X^2+1) &\cong \mathbb{Q}[-i] \subseteq \mathbb{C}.\end{aligned}$$

Então, pelo argumeto apresentado, obtemos a seguinte relação:

$$(\text{numero de hom. injetor } \mathbb{Q}[i] \to \mathbb{C}) = (\text{qtd. de raizes distintas de } X^2+1).$$

Agora, para cada $\psi : \mathbb{Q}[i] \to \mathbb{C}$, lembre-se que $\mathbb{Q}[i]$ contém todas as raízes de X^2+1. Isso significa que $\psi(i) \in \mathbb{Q}[i]$, e portanto, $\mathrm{Im}\,\psi \subseteq \mathbb{Q}[i]$. Como consequência, vale que $\psi \in \mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})$. Então $|\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})| = 2$, e $\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q}) = \{1, \sigma\}$, em que $\sigma(a+bi) = a - bi$ é a conjugação complexa.

Por fim, assuma que começamos com o corpo $\mathbb{Q}[i]$ e o subgrupo $G = \{1, \sigma\} \subseteq \mathrm{Aut}(\mathbb{Q}[i])$ (na verdade, neste exemplo, vale que $G = \mathrm{Aut}(\mathbb{Q}[i])$). Para recuperar o corpo $\mathbb{Q}$, podemos considerar o corpo fixo por G:

$$\mathbb{Q}[i]^G = \{\alpha \in \mathbb{Q}[i] \mid \psi(\alpha) = \alpha, \forall \psi \in G\} = \mathbb{Q}.$$

Para esse caso especial, a relação acima se traduz em:

$$\mathbb{Q} = \{\alpha \in \mathbb{Q}[i] \mid \bar{\alpha} = \alpha\}.$$

3. **Exemplo:** $\mathbb{Q}[\sqrt[3]{2}]$**.** Considere o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e $\sqrt[3]{2}$:

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \mid a, b, c \in \mathbb{Q}\}.$$

Temos que $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] = 3$ é finita, e o elemento $\sqrt[3]{2}$ satisfaz um polinômio (por exemplo, $X^3 - 2$).

Temos que $\mathbb{Q}[\sqrt[3]{2}]$ é corpo, pois considere $\psi_{\sqrt[3]{2}} : \mathbb{Q}[X] \to \mathbb{C}$, dado por $\psi_{\sqrt[3]{2}}(X) = \sqrt[3]{2}$. Daí $\operatorname{Im}\psi_{\sqrt[3]{2}} = \mathbb{Q}[\sqrt[3]{2}]$, e $(X^3 - 2) \subseteq \ker\psi_{\sqrt[3]{2}}$. Além disso, $X^3 - 2$ é irredutível em $\mathbb{Q}[X]$ (por critério de Eisenstein, por exemplo). Daí $(X^3 - 2)$ é ideal maximal, e portanto, $\ker\psi_{\sqrt[3]{2}} = (X^3 - 2)$. Segue que

$$\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3 - 2)$$

é corpo.

O polinômio $X^3 - 2$ é mônico, irredutível em $\mathbb{Q}[X]$ e possui $\sqrt[3]{2}$ como uma de suas raízes. Portanto, $X^3 - 2$ será o polinômio minimal de $\sqrt[3]{2}$ sobre $\mathbb{Q}$.

As raízes de $X^3 - 2$ em $\mathbb{C}$ são $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ e $\omega^2\sqrt[3]{2}$, em que $\omega \neq \omega^3 = 1$. Daí, vale também:

$$\mathbb{Q}[\omega\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}[\omega^2\sqrt[3]{2}] \cong \mathbb{Q}[\sqrt[3]{2}].$$

Porém, esses corpos são distintos. Isso se deve ao fato que $\mathbb{Q}[\sqrt[3]{2}]$ NÃO contém todas as raízes de $X^3 - 2$ (de fato, $\mathbb{Q}[\sqrt[3]{2}]$ contém somente a única raiz real).

Vamos calcular $\operatorname{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$. Repetindo a ideia do caso $\mathbb{Q}[i]$, nós temos três inclusões $\mathbb{Q}[\sqrt[3]{2}] \to \mathbb{C}$. Porém, os conjuntos imagens são todos distintos. Portanto, a única possibilidade é que $\operatorname{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{1\}$.

Para finalizar, o seu corpo fixo será:

$$\mathbb{Q}[\sqrt[3]{2}]^{\operatorname{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})} = \{\alpha \in \mathbb{Q}[\sqrt[3]{2}] \mid \psi(\alpha) = \alpha, \forall\psi \in \operatorname{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})\} = \mathbb{Q}[\sqrt[3]{2}].$$

4. **Exemplo:** $\mathbb{Q}[\xi]$**,** $\xi \neq \xi^5 = 1$**.** Seja $\xi \in \mathbb{C}$ de modo que $\xi \neq \xi^5 = 1$. Chamamos tal elemento de uma 5-raiz primitiva da unidade. Note que, se $i \in \{1, 2, 3, 4\}$, então

$$(\xi^i)^5 = (\xi^5)^i = 1.$$

Note também que $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Seja $\Phi_5(X) := X^4 + X^3 + X^2 + X + 1$. Então, pelo visto acima, as raízes de $\Phi_5(X)$ são ξ, ξ^2, ξ^3, ξ^4. Além disso, $\Phi_5(X)$ é irredutível em $\mathbb{Q}[X]$ (exercício).

Seja $\mathbb{Q}[\xi] \subseteq \mathbb{C}$ o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e ξ. Note que as raízes de $\Phi_5(X)$ são $\xi, \xi^2, \xi^3, \xi^4 \in \mathbb{Q}[\xi]$. Assim sendo, sem descrever explicitamente o conjunto $\mathbb{Q}[\xi]$, responda:

(i) $\mathbb{Q}[\xi]$ é corpo?
(ii) $\dim_{\mathbb{Q}} \mathbb{Q}[\xi] = ?$
(iii) Quantos homomorfismos de anéis não-nulo $\mathbb{Q}[\xi] \to \mathbb{C}$ existem?
(iv) $|\operatorname{Aut}(\mathbb{Q}[\xi]/\mathbb{Q})| = ?$

5. **Exemplo: $\mathbb{Q}[\pi]$.** Sabe-se que π é um número transcendente (Lindemann, 1882), ou seja, π não é raiz de um polinômio não-nulo com coeficientes em $\mathbb{Q}$. Considere $\mathbb{Q}[\pi]$ o menor subanel de $\mathbb{C}$ contendo π e $\mathbb{Q}$. Temos que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = \infty$. De fato, assuma por absurdo que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = n < \infty$. Então 1, π, ..., π^n são $\mathbb{Q}$-linearmente dependentes. Daí, existem $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, não todos nulos, tais que $0 = a_0 + a_1\pi + \cdots + a_n\pi^n$. Isso implica que π é raiz do polinômio $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Q}[X]$, uma contradição.

Para descrever $\mathbb{Q}[\pi]$, considere o mapa $\psi_\pi : \mathbb{Q}[X] \to \mathbb{C}$ tal que $\psi_\pi(X) = \pi$. Então $\operatorname{Im}\psi_\pi = \mathbb{Q}[\pi]$, e $\ker\psi_\pi = 0$ (caso contrário, iríamos contradizer a transcendência de π). Do Teorema do Isomorfismo, segue que $\mathbb{Q}[X] \cong \mathbb{Q}[\pi]$. Portanto, $\mathbb{Q}[\pi]$ não é corpo, e

$$\mathbb{Q}[\pi] = \{a_0 + a_1\pi + \cdots + a_n\pi^n \mid n \in \mathbb{N},\, a_0, a_1, \ldots, a_n \in \mathbb{Q}\} = \{f(\pi) \mid f \in \mathbb{Q}[X]\}.$$

O menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}[\pi]$ é o seu corpo de frações, denotado por $\mathbb{Q}(\pi)$. Temos

$$\mathbb{Q}(\pi) \cong \mathbb{Q}(X) := \text{corpo de frações de } \mathbb{Q}[X].$$

Note que para qualquer outro elemento transcendente $\alpha \in \mathbb{C}$, por mesmo argumento, teríamos que $\mathbb{Q}[\alpha] \cong \mathbb{Q}[X]$. Então, temos infinitos (não-enumerável) monomorfismos $\mathbb{Q}(\pi) \to \mathbb{C}$.

Exercício. Dados $\alpha, \beta \in \mathbb{C}$ transcendentes (sobre $\mathbb{Q}$), o que podemos falar de $\mathbb{Q}[\alpha, \beta]$, o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$, α e β?

6. **Exemplo: corpos finitos.** Seja $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ o corpo com 2 elementos, e seja $\mathbb{F}_4$ o $\mathbb{F}_2$-espaço vetorial com base $\{1, y\}$. Então $\mathbb{F}_4 = \{0, 1, y, 1+y\}$. Considere o produto em $\mathbb{F}_4$ dado por

	0	1	y	$1+y$
0	0	0	0	0
1	0	1	y	$1+y$
y	0	y	$1+y$	1
$1+y$	0	$1+y$	1	y

Temos que $\mathbb{F}_4$ é um corpo. Uma forma de verificar é o seguinte: o polinômio X^2+X+1 é irredutível em $\mathbb{F}_2[X]$ (pois não possui raízes em $\mathbb{F}_2$). Então $\mathbb{F}_2[X]/(X^2+X+1)$ é um corpo com 4 elementos. Tome $y = X + (X^2 + X + 1)$. Verifica-se que o produto dos elementos em $\mathbb{F}_2[X]/(X^2 + X + 1)$ coincide com os da tabela. Daí

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1).$$

Exercícios.

(1) Construa um corpo com 9 elementos.
(2) Sejam $f_1 = X^3+X^2+1$ e $f_2 = X^3+X+1$. Prove que f_1 e f_2 são irredutíveis em $\mathbb{F}_2[X]$. Exiba um isomorfismo de corpos $\mathbb{F}_2[X]/(f_1) \to \mathbb{F}_2[X]/(f_2)$.

7. **Exemplo: Polinômio X^p quando $\operatorname{car}\mathbb{F} = p$.** Seja $\mathbb{F}$ um corpo finito e de característica $p > 0$. Então, dados $a, b \in \mathbb{F}$, vale que (verifique)

$$(a + b)^p = a^p + b^p.$$

Assim, seja $F : \mathbb{F} \to \mathbb{F}$ o mapa definido por $F(a) = a^p$. Temos que

$$F(a + b) = (a + b)^p = a^p + b^p = F(a) + F(b),$$
$$F(ab) = (ab)^p = a^pb^p = F(a)F(b).$$

Daí F é um homomorfismo de anéis. Além disso, $0 = F(a) = a^p$ implica $a = 0$, ou seja, F é um monomorfismo. No caso de $\mathbb{F}$ ser finito, temos então que $\mathbb{F}$ é também sobrejetiva. Assim, dado $a \in \mathbb{F}$, existe $b \in \mathbb{F}$ tal que $a = F(b) = b^p$. Portanto, o polinômio

$$f_a(X) = X^p - a = X^p - b^p = (X - b)^p$$

possui todas as raízes repetidas, e iguais a b.

Agora, considere $\mathbb{E} = \mathbb{F}(Y)$, o corpo de frações do anel de polinômios $\mathbb{F}[Y]$. Considere $f(X) = X^p - Y \in \mathbb{E}[X]$. Temos que não existe $b \in \mathbb{E}$ de modo que $b^p = Y$. Além disso, veremos que o tal polinômio f é irredutível.

Se existir um corpo $\mathbb{L} \supseteq \mathbb{E}$ (na verdade, sempre existe!) em que f possui raiz, então todas as raízes de f serão repetidas. Assim, f é um exemplo de um polinômio irredutível tal que

$$(\text{qtd. de raízes distintas de } f) < \text{gr}(f).$$

8. **Exemplo: $\mathbb{Q}[\sqrt{2}, i]$.** Considere o seguinte subanel de $\mathbb{C}$,

$$\mathbb{Q}[\sqrt{2}, i] = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}.$$

Temos $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] = 4$. Podemos escrever também $\mathbb{Q}[\sqrt{2}, i] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}[i]\}$, o que indica que $\mathbb{Q}[\sqrt{2}, i]$ não é somente um $\mathbb{Q}$-espaço vetorial, mas também um $\mathbb{Q}[i]$-espaço vetorial de dimensão 2 (já vimos que $\mathbb{Q}[i]$ é um corpo). Além disso, tal observação evidencia a seguinte fórmula:

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

Seria $\mathbb{Q}[\sqrt{2}, i]$ um corpo?

Dado $0 \neq r \in \mathbb{Q}[\sqrt{2}, i]$, então a multiplicação por r é uma transformação linear $L_r : \mathbb{Q}[\sqrt{2}, i] \to \mathbb{Q}[\sqrt{2}, i]$, $L_r(a) = ra$. Além disso, como $\mathbb{Q}[\sqrt{2}, i]$ é domínio (pois é um subanel de $\mathbb{C}$, que é corpo), segue que L_r é injetora. Como $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] < \infty$, segue que L_r é também sobrejetora. Portanto, existe $s \in \mathbb{Q}[\sqrt{2}, i]$ tal que $rs = L_r(s) = 1$. Isso implica que $r^{-1} = s \in \mathbb{Q}[\sqrt{2}, i]$, ou seja, $\mathbb{Q}[\sqrt{2}, i]$ é corpo.

Qual seria seu grupo de $\mathbb{Q}$-automorfismos?

Temos que $\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}) = \{\eta_0, \eta_1, \eta_2, \eta_3\}$, em que $\eta_0 = \text{Id}$, e

$$\eta_1(a + b\sqrt{2} + ci + d\sqrt{2}i) = a - b\sqrt{2} + ci - d\sqrt{2}i,$$
$$\eta_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} - ci - d\sqrt{2}i,$$
$$\eta_3 = \eta_1\eta_2.$$

Em outras palavras, $\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}) = \langle \eta_1, \eta_2 \rangle \cong C_2 \times C_2$. Perceba que cada elemento de $\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q})$ é unicamente descrito por sua ação em $\sqrt{2}$ e em i.

O corpo fixo, neste caso, é (verifique)

$$\mathbb{Q}[\sqrt{2}, i]^{\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}} = \mathbb{Q}.$$

Agora, vimos que $\mathbb{Q}[i] \subseteq \mathbb{Q}[\sqrt{2}, i]$. Então, conseguiríamos calcular o grupo dos $\mathbb{Q}[i]$-automorfismos, isto é, $\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}[i])$?

Dado $\psi \in \text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}[i])$, temos $\psi(\alpha) = \alpha$, $\forall \alpha \in \mathbb{Q}[i]$. Em particular, $\psi(\alpha) = \alpha$, $\forall \alpha \in \mathbb{Q}$. Daí, obtemos que

$$\text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}[i]) \subseteq \text{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}).$$

Assim sendo, ψ é unicamente determinado por sua ação sobre $\sqrt{2}$ e sobre i. Necessariamente temos que $\psi(i) = i$, e que $\psi(\sqrt{2}) \in \{sqrt2, -\sqrt{2}\}$. Além disso, as duas

possibilidades são possíveis de ocorrer. Assim, o tal grupo de automorfismos possui dois elementos. Mais precisamente, temos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[i]) = \{\eta_0, \eta_1\} = \langle \eta_1 \rangle \cong C_2.$$

Seu corpo fixo é

$$\begin{aligned}\mathbb{Q}[\sqrt{2},i]^{\langle \eta_1 \rangle} &= \{\alpha + \beta\sqrt{2} \in \mathbb{Q}[\sqrt{2},i] \mid \alpha + \beta\sqrt{2} = \eta_1(\alpha + \beta\sqrt{2}) = \alpha - \beta\sqrt{2}\} \\ &= \{\alpha \in \mathbb{Q}[i]\} = \mathbb{Q}[i].\end{aligned}$$

Agora, vamos fazer o contrário. Comecemos com o subgrupo $H_2 = \langle \eta_2 \rangle$. Então, o corpo fixo desse subgrupo é (verifique)

$$\mathbb{Q}[\sqrt{2},i]^{\langle \eta_2 \rangle} = \mathbb{Q}[\sqrt{2}].$$

Usando argumentos similares ao caso anterior, obtemos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[\sqrt{2}]) = \langle \eta_2 \rangle.$$

Por fim, temos um último subcorpo de $\mathbb{Q}[\sqrt{2},i]$, que é $\mathbb{Q}[\sqrt{2}i]$. Temos também um último subgrupo do grupo de autormosfismos, $H_3 = \langle \eta_1\eta_2 \rangle = \langle \eta_3 \rangle$. Ambos estão relacionados por

$$\mathbb{Q}[\sqrt{2},i]^{\langle \eta_3 \rangle} = \mathbb{Q}[\sqrt{2}i], \quad \mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[\sqrt{2}i]) = \langle \eta_3 \rangle.$$

Portanto, exibimos uma correspondência biunívoca entre os corpos $\mathbb{F}$, com $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}[\sqrt{2},i]$, e os subgrupos de $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q})$. Tal correspondência é um caso particular do Teorema Fundamental da Teoria de Galois.