Exemplo: $\mathbb{Q}[\pi]$

Sabe-se que π é um elemento transcendente sobre $\mathbb{Q}$ (Lindemann, 1882), ou seja, π não é raiz de um polinômio não nulo com coeficientes racionais.

Considere $\mathbb{Q}[\pi]$, o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e π. Temos que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = \infty$, de fato, assuma que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = n < \infty$. Então $\{1, \pi, \dots, \pi^n\}$ é um conjunto $\mathbb{Q}$-l.d, ou seja, existem $a_0, a_1, \dots, a_n$ racionais não todos nulos tais que

$$a_0 1 + a_1 \pi + \cdots + a_n \pi^n = 0,$$

Daí π satisfaz $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Q}[X]$, uma contradição.

Para descrever $\mathbb{Q}[\pi]$: considere $\Psi_\pi : \mathbb{Q}[X] \to \mathbb{C}$, dada por $\Psi_\pi(X) = \pi$. Então $\mathbb{Q}[\pi] = \operatorname{Im} \Psi_\pi$, e $\ker \Psi_\pi = 0$ (se não, contradiz o fato de π ser transcendente). Daí $\mathbb{Q}[\pi] \cong \mathbb{Q}[X]$, ou seja,

$$\mathbb{Q}[\pi] = \{a_0 + a_1 \pi + \cdots + a_n \pi^n \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in \mathbb{Q}\}.$$

O menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}$ e π é denotado

por $\mathbb{Q}(\pi)$, e $\mathbb{Q}(\pi) \cong \mathbb{Q}(X) = \text{corpo fr.}(\mathbb{Q}[X])$.

Dado outro $\alpha \in \mathbb{C}$ transcendente sobre $\mathbb{Q}$, teríamos que vale $\mathbb{Q}[\alpha] \cong \mathbb{Q}[X] \cong \mathbb{Q}[\pi]$.

Exemplo: corpos finitos

Seja $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ o corpo com 2 elementos. Seja $\mathbb{F}_4$ um $\mathbb{F}_2$-espaço vetorial com base $\{1, y\}$, então $\mathbb{F}_4 = \{0, 1, y, 1+y\}$. Considere o produto em $\mathbb{F}_4$:

$\cdot$	0	1	y	$1+y$
0	0	0	0	0
1	0	1	y	$1+y$
y	0	y	$y+1$	1
$1+y$	0	$1+y$	1	y

Alternativamente: o polinômio $X^2+X+1 \in \mathbb{F}_2[X]$ é irredutível (pois não possui raiz em $\mathbb{F}_2$). Então $\mathbb{F}_2[X]/(X^2+X+1)$ é corpo. Defina $y = X + (X^2+X+1)$, então $\mathbb{F}_2[X]/(X^2+X+1) = \{0, 1, y, 1+y\}$, e o produto de seus elementos coincide com a tabela acima. Daí $\mathbb{F}_4$ é corpo.

Exercícios:

1) Construa um corpo com 9 elementos.

2) Sejam $f_1 = X^3 + X^2 + 1$, $f_2 = X^3 + X + 1 \in \mathbb{F}_2[X]$.
Prove que f_1 e f_2 são irredutíveis em $\mathbb{F}_2[X]$.
Fatore o polinômio $f_2 = f_2(Y)$ em $\mathbb{F}_2[X]/(f_1)$.
Exiba um isomorfismo

$$\mathbb{F}_2[X]/(f_1) \longrightarrow \mathbb{F}_2[X]/(f_2).$$

Exemplo: X^p quando $\operatorname{car} \mathbb{F} = p$

Seja $\mathbb{F}$ um corpo finito de característica $p > 0$.

① Dados $a, b \in \mathbb{F}$, vale que

$$(a+b)^p = a^p + b^p \quad \text{(verifique)}.$$

② Defina $F: \mathbb{F} \to \mathbb{F}$ por $F(a) = a^p$. Temos

$$F(a+b) = (a+b)^p = a^p + b^p = F(a) + F(b),$$

$$F(ab) = (ab)^p = a^p b^p = F(a) \cdot F(b), \quad \forall a, b \in \mathbb{F}.$$

③ Daí F é um homomorfismo de anéis. Além disso, $0 = F(a) = a^p$ implica que $a = 0$, ou seja, F é injetiva.

Sendo $\mathbb{F}$ finito, implica que F também é sobrejetiva. Daí, dado $a \in \mathbb{F}$, existe $b \in \mathbb{F}$ tal que

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

Considere o polinômio $f_a(X) = X^p - a$. Note que

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

ou seja f_a admite todas as raízes repetidas.

Seja $\mathbb{E} = \mathbb{F}(Y)$ ($\mathbb{E}$ é um corpo infinito e $\operatorname{car} \mathbb{E} = p$). Considere

$$f(X) = X^p - Y \in \mathbb{E}[X].$$

Não existe $b \in \mathbb{E}$ tal que $b^p = Y$. Além disso, f é irredutível em $\mathbb{E}[X]$.

Se existir um corpo $\mathbb{L} \supseteq \mathbb{E}$ tal que f possui raiz em $\mathbb{L}$ (na verdade, existe), então todas as raízes de f serão repetidas. Ou seja, estamos na situação em que f é irredutível e

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

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

Considere o 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 $[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] = 4$. Podemos escrever

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

$$= \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}[i]\},$$

o que evidencia que $\mathbb{Q}[\sqrt{2}, i]$ é um $\mathbb{Q}[i]$-espaço vetorial de dimensão 2. Além disso, note que

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

Pergunta: $\mathbb{Q}[\sqrt{2}, i]$ é corpo?

Seja $0 \neq r \in \mathbb{Q}[\sqrt{2}, i]$. Então $\varphi_r : \mathbb{Q}[\sqrt{2}, i] \to \mathbb{Q}[\sqrt{2}, i]$ dada por $\varphi_r(a) = ra$. Temos que φ_r é transformação linear. Como $\mathbb{Q}[\sqrt{2}, i]$ é domínio (pois $\mathbb{C}$ é corpo), segue que φ_r é injetivo. Como $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] < \infty$, segue que φ_r também é sobrejetivo.

Daí, existe $s \in \mathbb{Q}[\sqrt{2}, i]$ tal que $1 = \varphi_r(s) = rs$, ou seja, $r^{-1} = s \in \mathbb{Q}(\sqrt{2}, i]$. Daí $\mathbb{Q}[\sqrt{2}, i]$ é corpo.

Afirmamos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}) = \{\eta_0, \eta_1, \eta_2, \eta_3\},$$

em que

$$\eta_0 = id,$$

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

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

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

Temos que $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}) = \langle \eta_1, \eta_2 \rangle \cong C_2 \times C_2$, além disso, podemos descrever assim

$$\eta_1(\sqrt{2}) = -\sqrt{2}, \quad \eta_1(i) = i,$$

$$\eta_2(\sqrt{2}) = \sqrt{2}, \quad \eta_2(i) = -i, \quad \eta_3 = \eta_1\eta_2.$$

Temos que $\mathbb{Q}[\sqrt{2}, i]^{\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q})} = \mathbb{Q}$.

Além disso, temos que $\mathbb{Q}[i] \subseteq \mathbb{Q}[\sqrt{2}, i]$, então o que seria

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}[i]) \ ?$$

Dado $\psi \in Aut(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q}[i])$, temos que

$$\psi(a+bi) = a+bi, \quad \forall\, a, b \in \mathbb{Q},$$

e, em particular, $\psi(a) = a$, $\forall\, a \in \mathbb{Q}$. Então

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

Verificando, obtemos que

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

além disso,

$$\mathbb{Q}[\sqrt{2}, i]^{\langle \eta_1 \rangle} = \mathbb{Q}[i].$$

Façamos o contrário, e seja $H = \langle \eta_2 \rangle$. Então

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

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

Vale também pro último subgrupo $\langle \eta_1 \eta_2 \rangle = \langle \eta_3 \rangle$ e subcorpo $\mathbb{Q}[\sqrt{2}\, i]$. Vale que

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

Assim, obtemos correspondência biunívoca entre corpos F, com $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}[\sqrt{2}, i]$ e subgrupos de $Aut(\mathbb{Q}[\sqrt{2}, i] / \mathbb{Q})$.

Isso é um caso particular do Teorema Fundamental da Teoria de Galois.