1. Extensão de corpos

Nosso interesse neste curso será estudar simetrias de um corpo, e uma boa forma de o fazer é estudando simetrias em relação a um subcorpo. Para tal propósito, será interessante dizermos como um corpo está incluso num segundo.

Uma noção didática de extensão de corpos é a seguinte:

Definição 1.1. Uma *extensão de corpos* $\mathbb{E}/\mathbb{F}$ é um par de corpos $\mathbb{E}$ e $\mathbb{F}$, com $\mathbb{F} \subseteq \mathbb{E}$.

Reforçamos que vai ser importante como um corpo é subconjunto de um outro corpo, e não somente vê-los como objetos abstratos.

Entretanto, faremos diversas construções em que formalmente um corpo não está contido no outro, porém existe um mapa injetivo entre os corpos. Então, para tais propósitos, a forma correta de definir extensão de corpos é a seguinte:

Definição 1.2. Uma *extensão de corpos* $\mathbb{E}/\mathbb{F}$ é uma tripla $(i, \mathbb{E}, \mathbb{F})$, em que $\mathbb{E}$ e $\mathbb{F}$ são corpos, e $i : \mathbb{F} \to \mathbb{E}$ é um homomorfismo injetor de anéis.

Ressaltamos que o homomorfismo i é a parte mais importante desta definição; pois um corpo $\mathbb{E}$ pode conter diversas cópias do corpo $\mathbb{F}$. Se identificarmos o corpo $\mathbb{F}$ com a imagem $i(\mathbb{F})$, então caímos na primeira definição. Vamos então, usar a Definição 1.1 para extensão de corpos, e sempre identificar o corpo com a sua imagem, se estivermos no caso da Definição 1.2.

Dada uma extensão de corpos $\mathbb{E}/\mathbb{F}$, temos que $\mathbb{E}$ é um espaço vetorial sobre o corpo $\mathbb{F}$. Sendo assim, definimos o seguinte:

Definição 1.3. O *grau* de uma extensão $\mathbb{E}/\mathbb{F}$, denotada por $[\mathbb{E} : \mathbb{F}]$, é a dimensão do espaço $\mathbb{E}$ sobre $\mathbb{F}$. Isto é, $[\mathbb{E} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E}$. Se $[\mathbb{E} : \mathbb{F}] < \infty$, dizemos que a extensão é *finita*. Dizemos que a extensão é quadrática, cúbica, etc... se a extensão tiver grau 2, 3, etc...

Exemplo 1.1.

(1) $\mathbb{C}/\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$. Uma base de $\mathbb{C}$ sobre $\mathbb{R}$ é $\{1, i\}$, em que $i^2 = -1$.
(2) $\mathbb{R}/\mathbb{Q}$ e $[\mathbb{R} : \mathbb{Q}] = \infty$ (por que?)
(3) Seja $\mathbb{F}_2$ o corpo com dois elementos (isto é, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$). Seja $\mathbb{E} = \mathbb{F}_2(X)$ o corpo de frações do anel de polinômios $\mathbb{F}_2[X]$. Então $[\mathbb{E} : \mathbb{F}_2] = \infty$.

    Se tomarmos $\mathbb{F}_2(Y)$ como sendo um outro corpo de frações do anel de polinômios, então claro que $\mathbb{F}_2(Y) \cong \mathbb{E}$. Entretanto, é possível ter outros homomorfismos injetores $\mathbb{F}_2(Y) \to \mathbb{E}$ (não necessariamente sobrejetores)? Nestes casos, quanto seria o grau da extensão $[\mathbb{E} : \mathbb{F}_2(Y)]$?

Teorema 1.4. *Considere extensões de corpos $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é finita se e só se $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são finitas. Além disso, neste caso, vale*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

No geral, se $\mathcal{E}$ é uma base de $\mathbb{E}$ sobre $\mathbb{F}$, e se $\mathcal{L}$ é uma base de $\mathbb{L}$ sobre $\mathbb{E}$, então $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{F}$.

Demonstração. Vamos provar a última afirmação do teorema, que terá como consequência as demais afirmações. Dado $\ell \in \mathbb{L}$, sendo $\mathcal{L}$ uma $\mathbb{E}$-base de $\mathbb{L}$, existem $a_1, \ldots, a_m \in \mathbb{E}$ e $\ell_1, \ldots, \ell_m \in \mathcal{L}$ de modo que

$$\ell = a_1\ell_1 + \cdots + a_m\ell_m.$$

Agora, para cada j, como $\mathcal{E}$ é uma $\mathbb{F}$-base de $\mathbb{E}$, existem $e_{j1}, \ldots, e_{jm_j} \in \mathcal{E}$ e $\alpha_{j1}, \ldots, \alpha_{jm_j} \in \mathbb{F}$ de modo que

$$a_j = \alpha_{j1}e_{j1} + \cdots + \alpha_{jm_j}e_{jm_j}.$$

Daí

$$\ell = \sum_{j=1}^{m}\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\ell_j.$$

Isso mostra que $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ gera o espaço $\mathbb{L}$ como um espaço vetorial sobre $\mathbb{F}$. Vamos provar que este conjunto é linearmente independente. Para tanto, considere uma $\mathbb{F}$-combinação linear dando zero:

$$0 = \sum_{j=1}^{m}\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\ell_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\right)\ell_j$$

Sendo os elementos $\sum_{i=1}^{m_j} \alpha_{ji}e_{ji} \in \mathbb{E}$ e $\mathcal{L}$ uma $\mathbb{E}$-base, segue que esses são nulos, ou seja, $\sum_{i=1}^{m_j} \alpha_{ji}e_{ji} = 0$. Mas, como cada $\alpha_{ji} \in \mathbb{F}$ e $\mathcal{E}$ é uma $\mathbb{F}$-base, segue que cada $\alpha_{ji} = 0$. Mas isso prova que os coeficientes iniciais são nulos, ou seja, $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ é de fato uma $\mathbb{F}$-base de $\mathbb{L}$. □

1.1. **Subanel gerado.** Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $S \subseteq \mathbb{E}$ um subconjunto. O *subanel* de $\mathbb{E}$, gerado por S sobre $\mathbb{F}$, é o menor subanel de $\mathbb{E}$ contendo $\mathbb{F}$ e S. Denota-se tal subanel por $\mathbb{F}[S]$. No caso em que $S = \{a_1, \ldots, a_m\}$ é finito, denota-se o subanel simplesmente por $\mathbb{F}[a_1, \ldots, a_m]$.

Exemplo 1.2.

(1) $\mathbb{C} = \mathbb{R}[i]$.
(2) Sendo $\pi \in \mathbb{R}$, temos que $\mathbb{Q}[\pi]$ consiste de todos os elementos da forma

$$\alpha_m\pi^m + \alpha_{m-1}\pi^{m-1} + \cdots + \alpha_1\pi + \alpha_0, \quad \alpha_0, \alpha_1, \ldots, \alpha_m \in \mathbb{Q}.$$

Então $\mathbb{Q}[\pi]$ é isomorfo ao anel de polinômios sobre $\mathbb{Q}$.

Questão 1.1. Por que "o menor subanel contendo tais elementos" existe? (dica: para a existência de um "menor subanel" contendo um subconjunto, é suficiente mostrar que a intersecção de uma família de subanéis ainda é um subanel. Por que?).

Exemplo 1.3. Nestas condições, em que $\mathbb{E}/\mathbb{F}$ e $S \subseteq \mathbb{E}$, mostre que

$$\mathbb{F}[S] = \left\{\sum_{i=1}^{m} \alpha_i a_{i_1} \cdots a_{i_r} \mid m \in \mathbb{N}, \alpha_i \in \mathbb{F}, a_{i_1}, \ldots, a_{i_r} \in S, r \in \mathbb{N}\right\},$$

ou seja, $\mathbb{F}[S]$ é constituído de todas as somas finitas de produto de elementos de $\mathbb{F} \cup S$.

Neste sentido, será importante para nós o seguinte resultado, e sua consequência:

Lema 1.5. *Seja $\mathcal{R}$ um domínio de integridade comutativo com unidade, contendo um corpo $\mathbb{F}$ como subanel, e assuma que as duas unidades coincidem. Se $\dim_{\mathbb{F}} \mathcal{R} < \infty$, então $\mathcal{R}$ é corpo.*

Demonstração. Por hipótese, temos que $\mathcal{R}$ é um anel comutativo com unidade 1. Então basta provarmos que os elementos não nulos de $\mathcal{R}$ são invertíveis. Seja $r \in \mathcal{R}$ não nulo. Considere o mapa $\varphi_r : \mathcal{R} \to \mathcal{R}$ definido por $\varphi_r(a) = ra$ (multiplicação por r). Então φ_r é uma transformação linear injetiva (pois $\mathcal{R}$ é um domínio). Sendo $\dim_{\mathbb{F}} \mathcal{R} < \infty$, segue que φ_r é sobrejetivo também. Isso significa que existe $s \in \mathcal{R}$ de modo que $1 = \varphi_r(s) = rs$, ou seja, r é invertível em $\mathcal{R}$. □

Corolário 1.6. *Sejam $\mathbb{E}/\mathbb{F}$ e $S \subseteq \mathbb{E}$. Se $\dim_{\mathbb{F}} \mathbb{F}[S]$ é finita, então $\mathbb{F}[S]$ é corpo.*

Demonstração. Por construção, $\mathbb{F}[S]$ é um anel comutativo contendo a mesma unidade de $\mathbb{F}$. Agora, sendo $\mathbb{F}[S]$ um subconjunto do corpo $\mathbb{E}$, segue que $\mathbb{F}[S]$ é um domínio de integridade. Ainda, por hipótese, $\dim_{\mathbb{F}} \mathbb{F}[S] < \infty$. Portanto, estamos na condição do teorema anterior, tomando $\mathcal{R} = \mathbb{F}[S]$. Concluí-se que $\mathbb{F}[S]$ é um corpo. □

Corolário 1.7. *Sejam $\mathbb{E}/\mathbb{F}$ finita e $S \subseteq \mathbb{E}$. Então $\mathbb{F}[S]$ é corpo.* □

1.2. **Subcorpo gerado.** Novamente, sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $S \subseteq \mathbb{E}$. O subcorpo gerado por S sobre $\mathbb{F}$, denotado por $\mathbb{F}(S)$, é o menor subcorpo de $\mathbb{E}$ contendo $\mathbb{F}$ e S. Se S for finito, digamos, $S = \{a_1, \ldots, a_m\}$, então denota-se o subcorpo gerado simplesmente por $\mathbb{F}(a_1, \ldots, a_m)$.

Questão 1.2. Por que existe um menor subcorpo?

Exemplo 1.4.

(1) Se $\mathbb{F}[S]$ já é corpo, então vale que $\mathbb{F}[S] = \mathbb{F}(S)$.
De fato, um argumento formal segue: como $\mathbb{F}(S)$ é também um subanel contendo $\mathbb{F}$ e S, segue que, por ser o menor, $\mathbb{F}[S] \subseteq \mathbb{F}(S)$ (esta continência sempre é verdadeira). Agora, como $\mathbb{F}[S]$ é um corpo e contém $\mathbb{F}$ e S, então, por ser o menor, $\mathbb{F}(S) \subseteq \mathbb{F}[S]$. Segue então que vale $\mathbb{F}(S) = \mathbb{F}[S]$.

(2) Seja $\pi \in \mathbb{R}$. Então $\mathbb{Q}(\pi)$ é isomorfo ao corpo de frações do anel de polinômios sobre $\mathbb{Q}$.

Definição 1.8. Uma extensão $\mathbb{E}/\mathbb{F}$ é dita ser *simples* se existe $\alpha \in \mathbb{E}$ de modo que $\mathbb{E} = \mathbb{F}(\alpha)$.

Exemplo 1.5.

(1) $\mathbb{C}/\mathbb{R}$ e $\mathbb{Q}(\pi)/\mathbb{Q}$ são exemplos de extensões simples. Perceba que podemos ter uma uma extensão simples de grau infinito ($[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$).

(2) Seria a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ simples? Note que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \right\}.$$

Por outro lado, considere o corpo $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Como $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, segue que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Agora,

$$\sqrt{2} = -\frac{1}{2}\left(\left(\sqrt{2} + \sqrt{3}\right)^2 - 5\right)\left(\sqrt{2} + \sqrt{3}\right) + 3\left(\sqrt{2} + \sqrt{3}\right) \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Além disso, $\sqrt{3} = \left(\sqrt{2} + \sqrt{3}\right) - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Daí obtemos que vale $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, e então, $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ é uma extensão simples.

Vamos finalizar a seção com uma construção. O nome dado para o corpo seguinte não é muito usual, porém a sua construção é bastante conhecida e essencial para a teoria (na verdade, não se preocupe com o nome, mas sim com a construção).

Definição 1.9. Seja $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$ um polinômio irredutível. Um *stem field de* $f(X)$ *sobre* $\mathbb{F}$ é um par $(\mathbb{E}, \alpha)$, em que $\mathbb{E}/\mathbb{F}$ é uma extensão de corpos, $\alpha \in \mathbb{E}$, $\mathbb{E} = \mathbb{F}(\alpha)$ e $f(\alpha) = 0$.

A existência de um tal par sempre existe, e a construção é a seguinte: sendo $f(X) \in \mathbb{F}[X]$ um polinômio irredutível, então o quociente $\mathbb{E} := \mathbb{F}[X]/(f(X))$ é um corpo. O elemento $\alpha = X + (f(X))$ é tal que $f(\alpha) = 0$ por construção. Além disso, segue da construção que $\mathbb{E} = \mathbb{F}[\alpha]$. Então o par $(\mathbb{F}[X]/(f(X)), X + (f(X)))$ satisfaz a Definição 1.9.
Exercício. Prove que o corpo $(\mathbb{E}, \alpha)$ satisfazendo a Definição 1.9 é único, a menos de isomorfismo.

Como consequência, temos o seguinte:

Teorema 1.10. *Sejam $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$. Então existe uma extensão de corpos $\mathbb{E}/\mathbb{F}$ em que $f(X)$ possui raiz em $\mathbb{E}$.*

Demonstração. Não há nada a fazer se $\mathrm{gr}(f) = 1$. Caso contrário, seja g uma componente irredutível de f. Pela construção anterior, o corpo $\mathbb{E} = \mathbb{F}[X]/(g(X))$ contém uma raiz de g, e portanto, uma raiz de f. □

Como consequência imediata, obtemos o seguinte:

Corolário 1.11. *Sejam $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$. Então existe uma extensão de corpos $\mathbb{E}/\mathbb{F}$ em que $f(X)$ possui todas as suas raízes em $\mathbb{E}$.* □