Grupos e Corpos

Prof. Lucas Calixto

Aula 10 - Fecho algébrico, Corpos de fatoração

Fecho algébrico

Seja uma extensão $\mathbb{F} \subset \mathbb{E}$

Até agora estudamos problemas do tipo: quando $\alpha \in \mathbb{E}$ é algébrico em $\mathbb{F}$?

$$\text{dado } \alpha \in \mathbb{E} \text{ queremos achar } f(x) \in \mathbb{F}[x] \text{ com } f(\alpha) = 0$$

Trocando o problema: quando $f(x) \in \mathbb{F}[x]$ tem raiz em $\mathbb{E}$?

$$\text{dado } f(x) \in \mathbb{F}[x] \text{ queremos achar } \alpha \in \mathbb{E} \text{ com } f(\alpha) = 0$$

O conjunto $\{\alpha \in \mathbb{E} \mid \alpha \text{ é algébrico sobre } \mathbb{F}\}$ é o fecho algébrico de $\mathbb{E}$ sobre $\mathbb{F}$

Teorema: O fecho algébrico de $\mathbb{E}$ sobre $\mathbb{F}$ é subcorpo de $\mathbb{E}$

Prova: Sejam $\alpha, \beta \in \mathbb{E}$ algébricos sobre $\mathbb{F}$

$\mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha)(\beta)$ é extensão finita de $\mathbb{F}$, pois $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}(\alpha, \beta)$ são extensões finitas $\Rightarrow \mathbb{F} \subset \mathbb{F}(\alpha, \beta)$ é extensão algébrica

Logo, $\alpha \pm \beta$, $\alpha\beta$ e α/β, por serem elementos de $\mathbb{F}(\alpha, \beta)$, são todos algébricos sobre $\mathbb{F}$
■

$\mathbb{F}$ é dito algebricamente fechado se todas as raízes de polis em $\mathbb{F}[x]$ vivem em $\mathbb{F}$

Nesse caso, se $f(x) \in \mathbb{F}[x]$ e $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ são as raízes de $f(x)$, então

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \text{ em } \mathbb{F}[x]$$

Corolário: Se $\mathbb{F}$ é algebricamente fechado e $\mathbb{F} \subset \mathbb{E}$ é extensão algébrica, então $\mathbb{E} = \mathbb{F}$

Temos agora 2 resultados super famosos

Teorema: Todo corpo admite uma única extensão $\mathbb{E}$ para a qual todas as raízes de polinomios em $\mathbb{F}[x]$ vivem em $\mathbb{E}$

Teorema fundamental da álgebra (TFA): $\mathbb{C}$ é algebricamente fechado

Prova: Vamos provar no próximo capítulo

Note: Gauss provou TFA em sua tese de doutorado

Corpos de fatoração

Se $p(x) \in \mathbb{F}[x]$ é não constante $\Rightarrow \exists$ extensão $\mathbb{F} \subset \mathbb{E}$ para a qual $p(x)$ tem raiz em $\mathbb{E}$

Vamos achar a menor extensão $\mathbb{E}$ para a qual $p(x)$ tem todas as raízes em $\mathbb{E}$

Note: se $\mathbb{E}$ é tal extensão e $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ são as raízes de $p(x)$, então é claro que $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ e que

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n) \text{ em } \mathbb{E}[x]$$

Tal corpo $\mathbb{E}$ é chamado de corpo de fatoração de $p(x)$

Nesse caso, dizemos também que $p(x)$ se fatora em fatores lineares em $\mathbb{E}[x]$

Exemplo: $p(x) = x^4 + 2x^2 - 8 \in \mathbb{Q}[x] \Rightarrow p(x) = (x^2 - 2)(x^2 + 4)$

Logo, as raízes de $p(x)$ são $\pm\sqrt{2}, \pm 2i$. Todas vivem em $\mathbb{Q}(\sqrt{2}, i)$ que é o corpo de decomposição de $p(x)$

Exemplo: $p(x) = x^3 - 3 \in \mathbb{Q}[x]$ tem raiz em $\mathbb{Q}(\sqrt[3]{3})$, mas esse não é o corpo de decomposição de $p(x)$, pois as outras raízes são complexas e obviamente não vivem em $\mathbb{Q}(\sqrt[3]{3})$

Note: para achar o corpo de fatoração de poli redutível $p(x) \in \mathbb{F}[x]$, digamos $p(x) = p_1(x)p_2(x)$ com $p_1(x)$ e $p(2)$ irredutíveis, basta acharmos primeiro corpo de fatoração $\mathbb{E}_1$ de $p_1(x) \in \mathbb{F}[x]$. Dai,

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_k)p_2(x) \text{ em } \mathbb{E}_1[x]$$

Agora achamos o corpo de fatoração $\mathbb{E}_2$ de $p_2(x) \in \mathbb{E}_1[x]$, dai $\mathbb{F} \subset \mathbb{E}_1 \subset \mathbb{E}_2$ e $\mathbb{E}_2$ é corpo de fatoração de $p(x)$

Teorema: Todo $p(x) \in \mathbb{F}[x]$ não constante admite corpo de fatoração $\mathbb{E}$

Prova: Indução em $\text{gr}(p(x))$. $\text{gr}(p(x)) = 1 \Rightarrow \mathbb{E} = \mathbb{F}$

Suponha $\text{gr}(p(x)) = n$ e que o resultado valha para todo poli de grau $< n$

Sabemos que existe $\mathbb{K} \supset \mathbb{F}$ para o qual $p(x)$ tem raiz α em $\mathbb{K}$. Logo

$$p(x) = (x - \alpha)q(x) \text{ em } \mathbb{K}[x]$$

Como $\text{gr}(q(x)) < n$, este admite corpo de fatoração $\mathbb{E}$ ($q(x) \in \mathbb{K}[x] \Rightarrow \mathbb{K} \subset \mathbb{E}$)

Logo, $\mathbb{E}$ é corpo de fatoração de $p(x)$ ■

Vamos ver que o corpo de fatoração de um poli em $\mathbb{F}[x]$ é único, em um certo sentido

Lema: Seja $\phi : \mathbb{E} \to \mathbb{F}$ um isomorfismo. Seja $\mathbb{E} \subset \mathbb{K}$ uma extensão e $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{K}$, com poli minimal $m_\alpha(x) = e_0 + e_1 x + \cdots + e_n x^n \in \mathbb{E}[x]$. Seja $\mathbb{F} \subset \mathbb{L}$ uma extensão onde o poli $m_\alpha^\phi(x) = \phi(e_0) + \phi(e_1)x + \cdots + \cdots \phi(e_n)x^n \in \mathbb{F}[x]$ tenha raiz $\beta \in \mathbb{L}$. Então ϕ se extende a um único iso $\bar{\phi} : \mathbb{E}(\alpha) \to \mathbb{F}(\beta)$ tal que $\bar{\phi}|_{\mathbb{E}} = \phi$ e $\bar{\phi}(\alpha) = \beta$.

Prova: Lembre que $\mathbb{E}(\alpha)$ é $\mathbb{E}$-espaço vetorial com base $\{1, \alpha, \ldots, \alpha^{n-1}\}$

Afirmação: o iso $\bar{\phi} : \mathbb{E}(\alpha) \to \mathbb{F}(\beta)$ será a a transformação linear

$$\bar{\phi}(e_0 + e_1\alpha + \cdots + e_n\alpha^{n-1}) = \phi(e_0) + \phi(e_1)\beta + \cdots + \phi(e_{n-1})\beta^{n-1}$$

Vamos ver que $\bar{\phi}$ é composição de isos

Verifiquem que $\phi : \mathbb{E}[x] \to \mathbb{F}[x]$, $f(x) \mapsto f^\phi(x)$ é um iso de aneis. Lembrem:

- $\mathbb{E}(\alpha) \cong \mathbb{E}[x]/\langle m_\alpha(x)\rangle$ e que $\mathbb{F}(\beta) \cong \mathbb{F}[x]/\langle m_\alpha^\phi(x)\rangle$ (note que $m_\alpha^\phi(x) = m_\beta(x)$)
- Tais isos são induzidos pelos homomorfismos de avaliação

$\sigma : \mathbb{E}[x]/\langle m_\alpha(x)\rangle \to \mathbb{E}(\alpha), \quad \sigma(f(x) + \langle m_\alpha(x)\rangle) = f(\alpha)$

$\tau : \mathbb{F}[x]/\langle m_\alpha^\phi(x)\rangle \to \mathbb{F}(\beta), \quad \tau(g(x) + \langle m_\alpha^\phi(x)\rangle) = g(\beta)$

- Como $\phi : \mathbb{E}[x] \to \mathbb{F}[x]$ é iso, e $\phi(m_\alpha(x)) = m_\alpha^\phi(x)$, então

$$\psi : \mathbb{E}[x]/\langle m_\alpha(x)\rangle \to \mathbb{F}[x]/\langle m_\alpha^\phi(x)\rangle, \quad f(x) + \langle m_\alpha(x)\rangle \mapsto f^\phi(x) + \langle m_\alpha^\phi(x)\rangle$$

é iso também

Combinando tudo, temos o diagrama comutativo

$$\begin{array}{ccc}
\mathbb{E}[x]/\langle m_\alpha(x)\rangle & \xrightarrow{\psi} & \mathbb{F}[x]/\langle m_\alpha^\phi(x)\rangle \\
\Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle \tau} \\
\mathbb{E}(\alpha) & \xrightarrow[\bar{\phi}]{} & \mathbb{F}(\beta) \\
\Big\downarrow{\scriptstyle cte} & & \Big\downarrow{\scriptstyle cte} \\
\mathbb{E} & \xrightarrow[\phi]{} & \mathbb{F}
\end{array}$$

Logo, $\bar{\phi} = \tau\psi\sigma^{-1}$ pois

$$f(\alpha) \mapsto f(x) + \langle m_\alpha(x)\rangle \mapsto f^\phi(x) + \langle m_\alpha^\phi(x)\rangle \mapsto f^\phi(\beta)$$

Finalmente, se $\varphi : \mathbb{E}(\alpha) \to \mathbb{F}(\beta)$ é iso tal que $\varphi|_{\mathbb{E}} = \phi$ e $\varphi(\alpha) = \beta$, então segue de álgebra linear que $\varphi = \bar{\phi}$ ■

Teorema: Seja $\phi : \mathbb{E} \to \mathbb{F}$ um isomorfismo, $p(x) \in \mathbb{E}[x]$ um poli não constante, e $p^{\phi}(x) \in \mathbb{F}[x]$. Se $\mathbb{K} \supset \mathbb{E}$ e $\mathbb{L} \supset \mathbb{F}$ são os corpos de fatoração de $p(x)$ e $p^{\phi}(x)$, então ϕ se extende a um único iso $\bar{\phi} : \mathbb{K} \to \mathbb{L}$.

Prova: Indução sobre $\text{gr}(p(x)) = n$

Podemos assumir que $p(x)$ é irredutível

Se $\text{gr}(p(x)) = 1 \Rightarrow \mathbb{K} = \mathbb{E}$ e não temos o que provar

Suponha que o resultado valha para todo poli de grau $< n$

Tome $\alpha \in \mathbb{K}$ raiz de $p(x)$ e $\beta \in \mathbb{L}$ raiz de $p^{\phi}(x)$

Note que $\mathbb{E} \subset \mathbb{E}(\alpha) \subset \mathbb{K}$ e $\mathbb{F} \subset \mathbb{F}(\beta) \subset \mathbb{L}$

lema $\Rightarrow$ existe único iso $\bar{\phi} : \mathbb{E}(\alpha) \to \mathbb{F}(\beta)$ estendendo ϕ tal que $\bar{\phi}(\alpha) = \beta$

$p(x) = (x - \alpha)f(x) \in \mathbb{E}(\alpha)[x] \Rightarrow p^{\phi}(x) = (x - \beta)f^{\phi}(x) \in \mathbb{F}(\beta)[x]$. Note:

- $\mathbb{K}$ também é corpo de fatoração de $f(x)$ sobre $\mathbb{E}(\alpha)$
- $\mathbb{L}$ também é corpo de fatoração de $f^{\phi}(x)$ sobre $\mathbb{F}(\beta)$

$\text{gr}(f(x)) < n \Rightarrow$ existe único iso $\psi : \mathbb{K} \to \mathbb{L}$ extendendo $\bar{\phi}$ (e portanto ϕ) ■

Agora temos a unicidade de corpos de fatoração

Corolário Todo poli $p(x) \in \mathbb{F}[x]$ admite corpo de fatoração, o qual é único a menos de isomorfismo que deixa fixo os elementos de $\mathbb{F}$

Prova: Sejam $\mathbb{K}$ e $\mathbb{L}$ dois corpos de fatoração de $p(x)$

Então, estamos na situação do ultimo teorema com $\phi = \text{id} : \mathbb{F} \to \mathbb{F}$, e portanto existe único iso $\bar{\phi} : \mathbb{K} \to \mathbb{L}$ tal que $\bar{\phi}|_{\mathbb{F}} = \text{id}$ (ou seja, que fixa os elementos de $\mathbb{F}$) ■

Corpos finitos

Já conhecemos corpos com ordem p, os $\mathbb{Z}_p$

Já sabemos construir alguns exemplos de corpos de ordem potência de p

Exemplo: $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ tem ordem $2^2 = 4$

Vamos ver que para cada primo p e $n \in \mathbb{N}$ existe um único corpo de ordem p^n, os chamados corpos de Galois

Lembre que $\operatorname{car}\mathbb{F} = p$ se $p\alpha = 0\ \forall \alpha \in \mathbb{F}$, ou equivalentemente, $\operatorname{car}\mathbb{F} = |1|$ em $(\mathbb{F}, +)$

Suponha $|F| = n = p_1 \cdots p_k$ (fatoração de n em primos com repetições permitidas). Então $n1 = (p_1 1) \cdots (p_k 1) = 0 \Rightarrow p_i 1 = 0$ para algum $i \Rightarrow \operatorname{car}\mathbb{F} = p_i$. Logo, temos

Proposição: Se $|F| < \infty$, então $\operatorname{car}\mathbb{F} = p$ com p primo

Proposição: Se $\operatorname{car}\mathbb{F} = p$, então $|F| = p^n$ para algum $n \in \mathbb{N}$

Prova: Segue do fato que $(\mathbb{F}, +)$ é um p-grupo ■

Obs: para todo corpo $\mathbb{F}$, temos que $\phi : \mathbb{Z} \to \mathbb{F}$, $\phi(n) = n$ é homomorfismo

Se $\operatorname{car} \mathbb{F} = p$, então $\ker \phi = p\mathbb{Z}$ e portanto $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \operatorname{im} \phi = \langle 1 \rangle_+ \leq (\mathbb{F}, +)$

Se $|\mathbb{F}| < \infty$, então $\mathbb{Z}_p \subset \mathbb{F}$ é extensão finita, digamos $[\mathbb{F} : \mathbb{Z}_p] = n$ com base $\alpha_1, \ldots, \alpha_n$. Então

$$\mathbb{F} = \{a_1\alpha_1 + \cdots + a_n\alpha_n \mid a_i \in \mathbb{Z}_p\} \Rightarrow |\mathbb{F}| = p^n$$

Lema (Freshman's dream $\cong$ sonho de calouro) Seja p um primo e D um domínio integral com $\operatorname{car} D = p$, então

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

Prova: Exercício ■

Um poli $f(x) \in \mathbb{F}[x]$ é dito separável se todas as suas raízes são distintas. Nesse caso todos os fatores lineáres

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

no corpo de decomposição de $f(x)$ aparecem com multiplicidade 1

Uma extensão $\mathbb{F} \subset \mathbb{E}$ é separável se todo $\alpha \in \mathbb{E}$ é raiz de um poli separável de $\mathbb{F}[x]$

Exemplo: $p(x) = x^2 + 2 \in \mathbb{Q}[x]$ é separável, já que $p(x) = (x - \sqrt{2})(x + \sqrt{2})$ em $\mathbb{Q}(\sqrt{2})[x]$. Por outro lado, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ é extensão separável de $\mathbb{Q}$. De fato, seja $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ com $b \neq 0$ (caso contrário não tem o que provar). Se $\bar{\alpha} = a - b\sqrt{2}$, então α é raiz de

$$p(x) = (x - \alpha)(x - \bar{\alpha}) \in \mathbb{Q}[x] \quad \text{(verifique)}$$

Um método para verificar se um poli $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ é separável faz uso de sua derivada (formal)

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in \mathbb{F}[x]$$

Lema: $f(x) \in \mathbb{F}[x]$ é separável $\Leftrightarrow mdc(f(x), f'(x)) = 1$

Prova: ($\Rightarrow$): se $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, então

$$f'(x) = (x-\alpha_2) \cdots (x-\alpha_n) + (x-\alpha_1)(x-\alpha_3) \cdots (x-\alpha_n) + (x-\alpha_1)(x-\alpha_3) \cdots (x-\alpha_{n-1})$$

$\Rightarrow mdc(f(x), f'(x)) = 1$

($\Leftarrow$) : $f(x)$ não separável $\Rightarrow f(x) = (x - \alpha)^k g(x)$ para $k > 1$. Logo,

$$f'(x) = k(x - \alpha)^{k-1} g(x) + (x - \alpha)^k g'(x) \Rightarrow mdc(f(x), f'(x)) \neq 1$$

■

Lema: Sejam p primo, $n \in \mathbb{N}$ e $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Então o corpo de fatoração $\mathbb{F}$ de $f(x)$ (sobre $\mathbb{Z}_p$) tem ordem p^n

Prova: Sabemos que $f(x)$ tem p^n raízes (a principio, pode ter repetições). Sejam elas $R = \{\alpha_1, \ldots, \alpha_k\}$

Então $\mathbb{Z}_p \subset \mathbb{F} = \mathbb{Z}_p(\alpha_1, \ldots, \alpha_k) \Rightarrow [\mathbb{F} : \mathbb{Z}_p] = \ell < \infty \Rightarrow |\mathbb{F}| = p^\ell \Rightarrow \operatorname{car} \mathbb{F} = p$

$f'(x) = p^n x^{p^n - 1} - 1 = -1 \Rightarrow mdc(f(x), f'(x)) = 1 \Rightarrow f(x)$ é separável $\Rightarrow k = p^n$

Afirmamos que R é um subcorpo de $\mathbb{F}$, e portanto $\mathbb{F} = R$ (sendo $\mathbb{F}$ o corpo de decomposição de $f(x)$). Se $\alpha, \beta \in R$, então $\alpha^{p^n} = \alpha$ e $\beta^{p^n} = \alpha$. Assim

- $f(\alpha - \beta) = (\alpha - \beta)^{p^n} - (\alpha - \beta) = \alpha^{p^n} + (-1)^{p^n} \beta^{p^n} - \alpha + \beta = (-1)^{p^n} \beta + \beta = 0$

$\Rightarrow \alpha - \beta \in R \Rightarrow (R, +)$ é subgrupo de $(\mathbb{F}, +)$

- $f(1) = 1^{p^n} - 1 = 0 \Rightarrow 1 \in R$
- $f(\alpha\beta) = (\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n} \beta^{p^n} - \alpha\beta = 0 \Rightarrow \alpha\beta \in R$
- $f(\alpha^{-1}) = (\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0 \Rightarrow \alpha^{-1} \in R$ ■

Teorema: Se $|\mathbb{F}| = p^n$, então $\mathbb{F}$ é corpo de fatoração de $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$

Prova: Nesse caso, sabemos que car $F = p$, e obs do slide 11 $\Rightarrow \mathbb{Z}_p \subset \mathbb{F}$ é extensão finita com $[\mathbb{F} : \mathbb{Z}_p] = n$

Seja $\alpha \in \mathbb{F}$. Se $\alpha = 0 \Rightarrow f(\alpha) = 0$

Se $\alpha \neq 0 \Rightarrow \alpha \in (\mathbb{F}^*, \cdot)$ (grupo multiplicativo) e portanto $\alpha^{p^n - 1} = 1$ (elemento identidade desse grupo). Ou seja, $\alpha^{p^n} - \alpha = 0 \Rightarrow f(\alpha) = 0$

Logo, todos os p^n elementos de $\mathbb{F}$ são raízes de $f(x) \Rightarrow f(x)$ se fatora em $\mathbb{F}$

Como $|\mathbb{F}| = p^n = |\text{raízes de } f(x)| \Rightarrow \mathbb{F}$ é corpo de fatoração de $f(x)$ ■

O único corpo de ordem p^n chamado de corpo de Galois de ordem p^n e é denotado por $GF(p^n)$

Teorema: Se $\mathbb{F} \subset GF(p^n)$, então $\mathbb{F} = GF(p^m)$ para algum m que divide n. Reciprocamente, para cada m que divide n temos que $GF(p^m) \subset GL(p^n)$

Prova: $\mathbb{F} \subset GF(p^n) \Rightarrow |F| = p^m$, pois $(F, +) \leq (GF(p^n), +)$

Então, $\mathbb{Z}_p = \langle 1 \rangle_+ \subset \mathbb{F} \subset GF(p^n)$ e portanto

$$n = [GF(p^n) : \mathbb{Z}_p] = [GF(p^n) : \mathbb{F}][\mathbb{F} : \mathbb{Z}_p] = [GF(p^n) : \mathbb{F}]m \Rightarrow m \mid n$$

Reciprocamente,

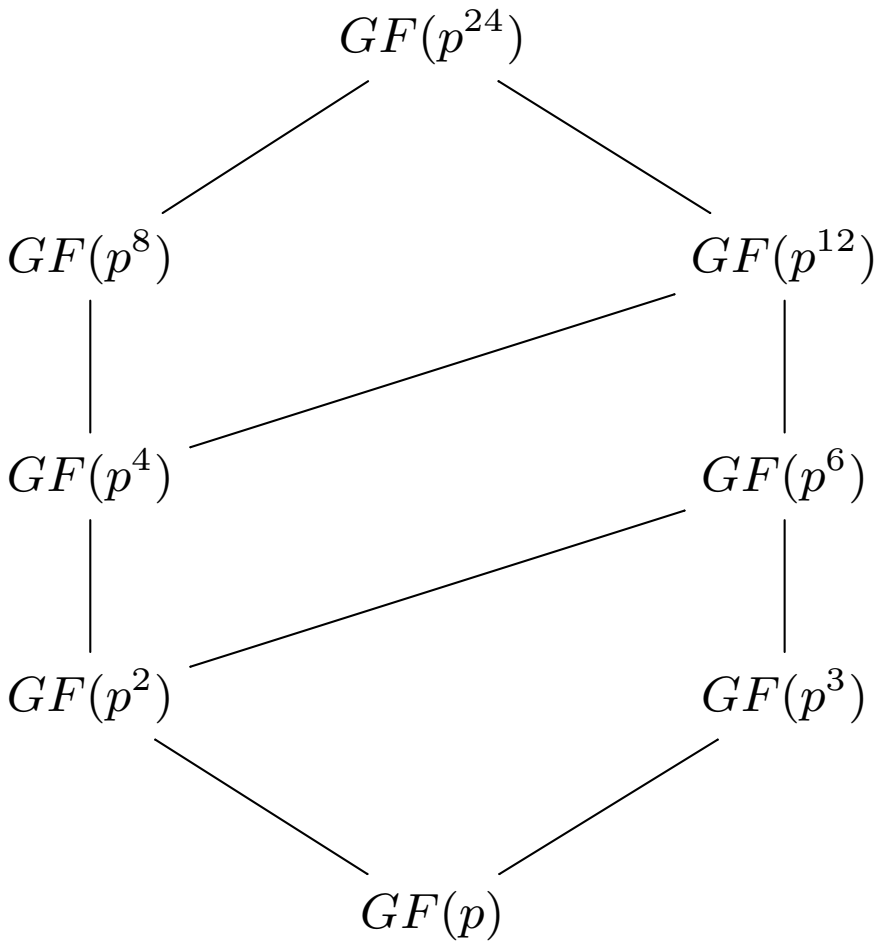
$$m \mid n \Rightarrow x^{p^m} - x \mid x^{p^n} - x \text{ em } \mathbb{Z}_p[x] \qquad \text{(detalhem)}$$

Logo, $GF(p^n)$ contem todas as raízes de $x^{p^m} - x \Rightarrow GF(p^n)$ contem um corpo de decomposição de $x^{p^m} - x$

Teorema anterior $\Rightarrow$ tal corpo é isomorfo a $GF(p^m)$, e sendo assim podemos pensar que $GF(p^m) \subset GF(p^n)$

Exercício: Todo poli $f(x) \in \mathbb{F}[x]$ pode ser considerado como uma função $f(x) : \mathbb{F} \to \mathbb{F}$, $f(x)(a) = f(a)$. É verdade que $f(x) = 0$ em $\mathbb{F}[x]$ se e só se a função $f(x)$ é identicamente nula (isto é, $f(a) = 0$ para todo $a \in \mathbb{F}$)?

Exemplo: O reticulado de subcorpos de $GF(p^{24})$ é o seguinte



O grupo $\mathbb{F}^*$

Denotamos o grupo multiplicativo $(\mathbb{F} \setminus \{0\}, \cdot)$ por $\mathbb{F}^*$

Teorema: Se $G \leq \mathbb{F}^*$ e $|G| < \infty$, então G é cíclico

Prova: Se $|G| = n$, então pelo TGA, temos

$$G \cong \mathbb{Z}_{p_1^{\epsilon_1}} \times \cdots \times \mathbb{Z}_{p_k^{\epsilon_k}},$$

onde $n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$

Afirmamos que $g = (e_1, \ldots, e_k)$ gera G (e_j é o gerador de $\mathbb{Z}_{p_j^{\epsilon_j}}$). De fato, seja $m = |g|$, então

$$m = mmc(|e_1|, \ldots, |e_k|) = mmc(p_1^{\epsilon_1}, \ldots, p_k^{\epsilon_k})$$

$\alpha = (a_1, \ldots, a_k) = (e_1^{a_1}, \ldots, e_k^{a_k}) \in G$ (na notação geral de grupos). Assim,

$$|\alpha| = mmc\left(|e_1^{a_1}|, \ldots, |e_k^{a_k}|\right) = mmc\left(\frac{|e_1|}{mdc(|e_1|, a_1)}, \ldots, \frac{|e_k|}{mdc(|e_k|, a_k)}\right)$$

$$= mmc\left(\frac{p_1^{\epsilon_1}}{mdc(p_1^{\epsilon_1}, a_1)}, \ldots, \frac{p_k^{\epsilon_k}}{mdc(p_k^{\epsilon_k}, a_k)}\right) \text{ que divide } m = mmc(p_1^{\epsilon_1}, \ldots, p_k^{\epsilon_k})$$

Logo, $\alpha^m = 1 \Rightarrow$ todo elemento de G é raiz de $x^m - 1 \Rightarrow n = |G| \leq m$

Mas, $m = |g| \leq |G| = n \Rightarrow m = n \Rightarrow G = \langle g \rangle$

Corolário: Se $|\mathbb{F}| < \infty$, então $\mathbb{F}^*$ é cíclico

Corolário: Sejam $\mathbb{E}$ e $\mathbb{F}$ corpos finitos tais que $\mathbb{F} \subset \mathbb{E}$ é extensão. Então $\mathbb{E}$ é extensão simples de $\mathbb{F}$

Prova: $\exists\ \alpha \in \mathbb{E}^*$ tal que $\mathbb{E}^* = \langle \alpha \rangle$. Como $\langle \alpha \rangle \subset \mathbb{F}(\alpha) \Rightarrow \mathbb{E} \subset \mathbb{F}(\alpha) \Rightarrow \mathbb{E} = \mathbb{F}(\alpha)$

Exemplo: $\mathbb{Z}_2/\langle x^4 + x + 1 \rangle$ é corpo com 2^4 elementos. Logo, se α é raiz de $x^4 + x + 1$ visto como elemento de $\mathbb{Z}_2/\langle x^4 + x + 1 \rangle[x]$, temos que

$$GF(2^4) \cong \mathbb{Z}_2/\langle x^4 + x + 1 \rangle = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in \mathbb{Z}_2\}$$

Como $GF(2^4) = \mathbb{Z}_2(\alpha)$, temos que $GF(2^4)^* = \langle \alpha \rangle$

Note: $|\alpha| = |GF(2^4)^*| = |GF(2^4) \setminus \{0\}| = 16 - 1 = 15$

$1 + \alpha + \alpha^4 = 0 \Rightarrow \alpha^4 = 1 + \alpha \Rightarrow \alpha^5 = \alpha + \alpha^2 \Rightarrow \cdots$ (complete)

Lista de exercícios

Cap 21: 3, 16, 18, 21

Cap 22: 1, 2, 3, 4, 5, 6, 8, 12, 13, 16, 17, 18, 19, 20, 21, 22