Capítulo 10 (pg. 321)

Aneis ⇒ Dominios $\nearrow$ I primo $\quad D/I$ domínio

$\searrow$ M maxima $\quad D/M$ corpo

Dominio ⇔ $\begin{cases} \cdot \text{ Anel} \\ \cdot \text{ com unidade} \\ \cdot \text{ comutativo} \\ \cdot \text{ Sem divisores de zero} \end{cases}$

exemplo fundamental $\mathbb{Z}$

Teorema fundamental da Aritmética: Todo inteiro ≥ 2 é produto de primo de forma única. (Um número p é primo os únicos divisores positivos são 1 e p $(p \neq 1)$)

Observação: se a divide b então $a \leq b$ (a e b positivos)

Prova: $n = 2$ como menores ou iguais a 2 são $1, 2$ e são os divisores ⇒ 2 é primo

H.I: Suponhamos que existe um n tal que para todo $2 \leq k < n$ temos que k é produto de primo

Dois casos:

Passo Indutivo: • Se n não é por nenhum número $2 \leq K < n$ $\Rightarrow$ os únicos divisores de n são 1 e n $\Rightarrow$ n é primo

- Se $\exists\, 2 \leq \underline{K} < n$ ✓ tal qe K divide n

$\Rightarrow$ $n = K \cdot m$ com $m = \frac{n}{K} \in \mathbb{Z}$

$\Rightarrow$ $2 \leq \underline{m} < n$ ✓

Por HJ tanto K com m são produto de primos $\Rightarrow$ $K \cdot m$ também é.

unicidade: Se $n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r$

i.e. n se pode escrever como produto de primos de duas formas distintas, além disso, podemos supor <u>n mínimo</u> com esta propriedade

(divide)

$p_1 \mid n \Rightarrow p_1 \mid q_1 \dots q_r \Rightarrow \exists j \;\; p_1 \mid q_j$

mas como q_j é primo $\Rightarrow$ $p_1 = q_j$

$$\frac{n}{p_1} = \frac{n}{q_j} = \underbrace{p_2 p_3 \dots p_s}_{} = \underbrace{q_1 \cdots q_{j-1}\, q_{j+1} \dots q_r}_{}$$

Logo $\frac{n}{p_1}$ tem 2 fatorações distintas

Contradiz o fato de ter escolhido n mínimo

$\square$

Teorema 4.25: $f(x) = a_k x^k + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ $p \nmid a_k$, p primo

- Se $\bar{f}(x) \in \mathbb{Z}_p[x]$ é iredutível $\Rightarrow$ $f(x) \in \mathbb{Z}[x]$ é iredutível ✓
- Se $f(x) \in \mathbb{Z}[x]$ não é iredutível $\Rightarrow$ $\bar{f}(x) \in \mathbb{Z}_p[x]$ não é iredutível

Prova:

Se $f(x) = g(x)h(x)$ $\qquad g(x) = b_\ell x^\ell + \dots$

$\qquad h(x) = c_s x^s + \dots$

$g(x)h(x) = c_s b_\ell x^{s+\ell = k} + \dots$ $\qquad c_s b_\ell = a_k$

$p \nmid c_s b_\ell \Rightarrow p \nmid c_s$ e $p \nmid b_\ell$

$\Rightarrow \bar{f}(x) = \underline{\bar{g}(x)}\,\underline{\bar{h}(x)}$ $\quad \to \operatorname{grau}(\bar{g}(x)) = \ell$, $\quad \to \operatorname{grau}(\bar{h}(x)) = s$

$\Rightarrow \bar{f}(x)$ é redutível $\square$

Exemplo: $f(x) = 11x^5 + 8x^4 + 3x^2 + 4x + 7$ é iredutível em $\mathbb{Q}[x]$

$\bar{f}(x) \equiv \underbrace{x^5 + x^2 + 1}$ mod 2 $\qquad \mathbb{Z}_2[x]$

$\bar{f}(0) \equiv 1$ mod 2 ✓ $\quad \bar{f}(1) \equiv 1$ mod 2 ✓

Logo $\bar{f}(x)$ não pode-se fatorar como produto de um fator de grau 1 × fator de grau 4

Polinomios de grau 2 $\Rightarrow \begin{cases} x^2,\ x^2+1 & x^2+x+1 \\ x^2+x & \end{cases}$

$x^2 = x\cdot x$ $\quad$ $x^2+1 = (x+1)^2$ $\quad$ $x^2+x = x(x+1)$

Logo o único que precisamos cosiderar é

$\underbrace{x^2+x+1}$

$\boxed{-1 = 1 \mod 2}$

$$
\begin{array}{l|l}
x^5 \qquad + x^2 \quad + 1 & x^2+x+1 \\ \cline{2-2}
\underline{x^5+x^4+x^3} & x^3+x^2 \\
\quad x^4+x^3+x^2 & \\
\quad \underline{x^4+x^3+x^2} & \\
\qquad\qquad 0 \qquad + 1 &
\end{array}
$$

$$x^5+x^2+1 = (x^3+x^2)(x^2+x+1) + 1$$

x^5+x^2+1 é irredutível em $\mathbb{Z}_2[x]$

Algoritmo da divisão ($\mathbb{Z}$)

Sejam $a, b \in \mathbb{Z}$ $b>0$ então existem inteiros q e r tais que

$\boxed{a = qb + r}$ com $0 \le r < b$

Prova: $\mathcal{E} = \{ a - qb \in \mathbb{N} \mid q \in \mathbb{Z} \} \subseteq \mathbb{N}$

$\mathcal{E}$ tem elemento mínimo e seja $r \in \mathcal{E}$ mínimo, como $r \in \mathcal{E} \Rightarrow \exists q \in \mathbb{Z}$ tal que $r = a - qb \Rightarrow a = qb + r$

Suponhamos por contradição que $\underline{\underline{r \geq b}}$

- $0 \leq s := r - b$
- $s = a - qb - b = a - (q+1)b \in \mathbb{Z}$

mas $s = r - b < r$ contraditório pois r é mínimo $\square$

---

* Se $a_1, \dots, a_n$ dividem b então $mdc(a_1 \dots a_n) = b$

Lema de Bezout: dados $a, b \in \mathbb{Z}$ existem $s, t \in \mathbb{Z}$ tal que $as + bt = mdc(a\,b)$, i.e o $mdc(a,b)$ é combinação linear inteira de a, b

---

Domínios de Ideais Principais: D é chamado de domínio de ideais principais (D.I.P) se para todo ideal $I \subseteq D$ existe $a \in D$ tal que $I = (a)$

* $\mathbb{Z}$ é DIP pois $I = (a_1, \dots, a_n) \subseteq \mathbb{Z}$

existem $s_1 \dots s_n$ tal que

$$mdc(a_1 \dots a_n) = a_1 s_1 + a_2 s_2 + \dots + a_n s_n \in I$$

$(\mathrm{mdc}(a_1 \dots a_n)) \subseteq I$

mas $a_j \in (\mathrm{mdc}(a_1, \dots a_n))$ $\forall j$ Logo

todos os geradores de I estão em $(\mathrm{mdc}(a_1 \dots a_n))$

$\Rightarrow$ $I \subseteq (\mathrm{mdc}(a_1 \dots a_n))$ Logo são igual

$\Rightarrow$ I é um ideal principal.

Def: Dado D domínio denotamos por $U(D)$ o conjunto de elemento de D que tem inverso em D.

Def: Um elemento $a \in D^* \setminus U(D)$ é chamado de irredutível se $\nexists\, b, c \in D^* \setminus U(D)$ com $a = bc$.

Def: Um domínio D é chamado Domínio de fatoração única (DFU) se para todo elemento em $D^* \setminus U(D)$ ele se pode escrever como produto de irredutíveis de forma única (salvo ordem e unidades)

Def: Um domínio D é chamado de Domínio Euclideano se

- Existe uma função $\boxed{\rho : D^* \to \mathbb{N}}$ que satisfaz que $a \mid b$ então $\rho(a) \leq \rho(b)$

• Se $a, b \in D^*$ então existem $q, r \in D$ tal que
• $a = bq + r$
• $r = 0$ ou $\rho(r) < \rho(b)$

Os $\mathbb{Z}$ é um Dominio euclideano

Pegando $\rho(b) = |b|$

Exemplo $\mathbb{Q}[x]$ é dominio euclideano

$$\rho : \mathbb{Q}[x]^* \longrightarrow \mathbb{N}$$
$$\underbrace{f(x)}\longmapsto \deg(f)$$

Se $g(x) \mid f(x)$ $\quad f(x) = g(x)h(x)$

$$\deg(f(x)) = \deg(g(x)h(x)) = \deg(g(x)) + \deg(h(x))$$
$$\geq \deg(g(x))$$

Teorema: Dados polinomios não nulos $f(x), g(x) \in K[x]$ (K corpo) existem $q(x)$ e $r(x) \in K[x]$ $\quad g(x) \neq 0$

• $f(x) = q(x)g(x) + r(x)$

• $r(x) = 0$ ou $\underset{\rho}{\deg}(r(x)) < \deg(g(x))$

Prova: $\mathcal{C} = \{ f(x) - q(x) g(x) \mid q(x) \in K[x] \}$

$$\deg : \mathcal{C} \to \mathbb{N} \cup \{-\infty\}$$
$$h(x) \to \deg(h(x))$$

$\deg(0) := -\infty$

$\deg(\mathcal{C}) \subseteq \mathbb{N} \cup \{-\infty\}$ Logo tem elemento mínimo

Se $\min = -\infty \Rightarrow 0 \in \mathcal{C}$

$\exists\, q(x)$ tal que $f(x) - q(x) g(x) = 0$
$\Rightarrow$ $\qquad\qquad\qquad\qquad \overset{\shortparallel}{r(x)}$

Se $\min = l \geq 0 \Rightarrow \exists\, q(x) \in K[x]$ tal que

$$\deg(f(x) - q(x) g(x)) = l$$

definindo $\quad r(x) = f(x) - q(x) g(x)$

$\Rightarrow \quad \boxed{f(x) = q(x) g(x) + r(x)}$

falta mostrar que $\deg(r(x)) < \deg(g(x))$

Suponhamos por contradição que

$$\boxed{\deg(r(x)) \geq \deg(g(x))} \leftarrow$$

$r(x) = a_s x^s + a_{s-1} x^{s-1} + \dots + a_0 \quad$ com $\; a_s \neq 0$

$\deg(r(x)) = s$

$g(x) = b_t x^t + b_{t-1} x^{t-1} \dots + b_0 \quad$ com $\; b_t \neq 0$

$\deg(g(x)) = t$ e $\underline{s \geq t}$

$$\underbrace{\underline{r(x)} - a_s b_t^{-1} \underline{x}^{s-t} \underline{g(x)}} = (a_s x^s + a_{s-1} x^{s-1} + \dots + a_0)$$

$$- a_s b_t^{-1} x^{s-t} (b_t x^t + b_{t-1} x^{t-1} \dots + b_0)$$

$$= (a_{s-1} - a_s b_{t-1}) x^{s-1} + \dots$$

$\tilde{r}(x) = \underline{r(x)} - a_s b_t^{-1} x^{s-t} g(x)$ tem grau $\deg(\tilde{r}(x)) \leq s-1$

$$f(x) = q(x) g(x) + (\tilde{r}(x) + a_s b_t^{-1} x^{s-t} g(x))$$

$$f(x) - (q(x) + a_s b_t^{-1} x^{s-t}) g(x) = \tilde{r}(x)$$

$$\mathscr{C} \qquad \tilde{r}(x) \in \mathscr{C}$$

$$\deg(\tilde{r}(x)) \leq s-1 < s = \deg(r(x))$$

Contraditório

Conclusão: $K[x]$ é um domínio euclideano com a função deg

Pensar: • $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$ é um domínio eucliano! $\underline{\underline{\underline{\text{!}}}}$

• $\mathbb{Z}[\sqrt{2}] = \{a+\sqrt{2}b \mid a,b \in \mathbb{Z}\}$ é domínio euclidano

---

• $\mathbb{Z}[\sqrt{-5}]$ não é euclideano.
(Vamos provar mais para frente) $\Leftarrow$

• $\mathbb{Z}[\sqrt{-5}]$ não é DFU (Pensar)

$$U(\mathbb{Z}[\sqrt{2}]) = \{(1+\sqrt{2})^{\ell} \mid \ell \in \mathbb{Z}\}$$

$$(1+\sqrt{2})^{\ell}(-1+\sqrt{2})^{\ell} = -1+2 = 1$$