Em capítulos anteriores foram analisados estruturas em $\mathbb{Z}$ e anéis polinômiais $F[x]$ usando divisibilidade, unidades, associações e primos irredutíveis. Começamos definido estas concepções de modo geral em um conjunto de um domínio de integridade.

"R é um domínio de integridade"

Domínio de integridade não tem divisores de zero.

Temos $a, b \in R$, com $a \neq 0$. Dizemos que a divide b (ou a é um fator de b) e escrevemos:

$$a \mid b \text{ se } b = ac \text{ para qualquer } c \in R$$

Lembramos que um elemento $\underline{u}$ em R é uma unidade:

$uv = 1_R \quad \forall v \in R \longrightarrow$ as unidades em R são precisamente os divisores de 1_R.

Exemplo 1: Somente unidades em $\mathbb{Z}$: 1 e -1,

se F é um corpo, então as unidades nos anéis de polinômios $F[x]$ são polinômios constantes diferentes de zero.

Exemplo 2: O conjunto $\mathbb{Z}[\sqrt{2}]$.

$\mathbb{Z}[\sqrt{2}] = \{r + s\sqrt{2} \mid r, s \in \mathbb{Z}\}$, é um subanel de números reais. O elemento $(1+\sqrt{2})$ é a unidade em $\mathbb{Z}[\sqrt{2}]$, porque:

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

No anel do exemplo precedido é um dos muitos aneis similares que iremos frequentemente usar como exemplos.

Se d é um inteiro fixado, então isto é fácil de verificar que o conjunto $\mathbb{Z}[\sqrt{d}] = \{r + s\sqrt{d} \mid r, s \in \mathbb{Z}\}$ é um domínio de integridade e esta contido nos números complexos.

- Se $d \geq 0$, então $\mathbb{Z}[\sqrt{d}]$ é um subanel dos números reais.

- Quando $d = -1$, então o anel $\mathbb{Z}[\sqrt{-1}]$ é usualmente denotado por $\mathbb{Z}[i]$, é chamado de anel gaussiano de inteiros.

Temos $u \in R$ sendo uma unidade com inverso v, então $uv = 1_R$.

$$v = \frac{1}{u} \rightarrow uv = u \cdot \frac{1}{u} = 1_R$$

Para qualquer $b \in R$, temos que $u(vb) = (uv)b = 1_R b = b$. Portanto: a unidade divide cada elemento de R

Um elemento $a \in R$ está associado a $b \in R$, $a = bu$ para qualquer unidade u.
Agora, u tem um inverso:

$uv = 1_R$, e v também é unidade.

- Se $u = 1 \rightarrow a = bu = b.1 = b$
- Se $uv = 1_R \rightarrow u = v = 1$.
- $a = bu \rightarrow av = buv = b1_R = b$

Usa-se o fato para verificar que:

"a está associado a b, se e somente se b está associado a a", e

"$a \neq 0$ em R, é divisível por cada um associado"

Exemplo 3: Cada inteiro diferente de zero n tem exatamente 2 associação em $\mathbb{Z}$, n e $-n$. Se F é um corpo, a associação de $f(x) \in F[x]$ são múltiplos constantes diferentes de zero de $f(x)$.

No anel $\mathbb{Z}[\sqrt{2}]$, os elementos $\sqrt{2}$ e $(2-\sqrt{2})$ estão associados porque:

$$\sqrt{2} = (2-\sqrt{2})\underbrace{(1+\sqrt{2})}_{\text{unidade}} = \cancel{2} - \cancel{\sqrt{2}} + \cancel{2}\sqrt{2} - \cancel{2} = \sqrt{2}$$

Um elemento $p \in R$, com $p \neq 0$, é dito irredutível, se p não é unidade e os únicos divisores de p estão associados a ele e as unidades de R.

<u>Exemplo 4</u>: Os elementos irredutíveis em $\mathbb{Z}$ são exatamente os primos inteiros, porque os únicos divisores de um primo p são $\pm p$ (seus associados) e ± 1 (as unidades de $\mathbb{Z}$).

A definição de irredutível dada anteriormente é idêntica a definição de um polinômio irredutível no domínio de integridade $F[x]$, quando F é um corpo.

Dizemos que um polinômio não constante $f(x)$ é irredutível em $K[x]$ (ou irredutível sobre K) <u>se é impossível</u> expressar $f(x)$ como um produto $g(x)h(x)$ de dois polinômios $g(x)$ e $h(x)$ em $K[x]$, cujos graus são ambos maiores ou iguais a 1.

<u>Teorema 10.1</u>: Temos p sendo diferente de zero, elemento não unidade em um domínio de integridade R. Então p é irredutível se e somente se:

Sempre que $p = rs \to r$ ou s é uma unidade

<u>Domínios Euclidianos</u>: O algoritmo da divisão foi uma ferramenta chave em análise aritmética de ambos $\mathbb{Z}$ e $F[x]$.

1) Definição: Um domínio de integridade R é um domínio Euclidiano, se existe uma função δ de elementos diferentes de zero de R para inteiros não inteiros não negativos com estas propriedades:

i) Se a e b são elementos diferentes de zero em R, então $\delta(a) \leq \delta(ab)$

ii) Se $a, b \in R$ e $b \neq 0_R$, então existe $q, r \in R$ sendo que $a = bq + r$ e além disso $r = 0_R$ ou $\delta(r) < \delta(b)$.

Exemplo 5: Se F é um corpo, então o domínio polinomial $F[x]$ é um domínio Euclidiano com a função δ dada por $\delta(f(x)) = \deg$ de $f(x)$.

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

Provamos por i) e ii) é exatamente a divisão algorítmica.

Exemplo 6: $\mathbb{Z}$ é um domínio Euclidiano com a função δ dada por $\delta(a) = |a|$.

i) $|ab| = |a||b| \geq |a|$ para todo a e b diferente de zero. Se $a, b \in \mathbb{Z}$, com $b > 0$, então pelo algoritmo da divisão existem inteiros q e r sendo que:

$a = bq + r$ e $0 \leq r < b$.

Além disso se $r=0$, ou r e b são ambos positivos, temos o caso:

i) $\delta(r) = |r| = r < b = |b| = \delta(b)$

Portanto, a propriedade (ii) mantém quando $b>0$.

<u>Exemplo 7</u>: Iremos provar que o anel de inteiros gaussianos $\mathbb{Z}[i] = \{s + ti \mid s, t \in \mathbb{Z}\}$ é um domínio euclidiano com a função δ dada por:

$$\delta(s+ti) = s^2 + t^2$$

Desde que $s+ti = 0$ se e somente se ambos s e t são 0, e temos que $\delta(s+ti) \geq 1$ quando $s+ti \neq 0$.

Verifica-se que para qualquer $a = s+ti$ e $b = u + vi$ em $\mathbb{Z}[i]$, $\delta(ab) = \delta(a)\delta(b)$.

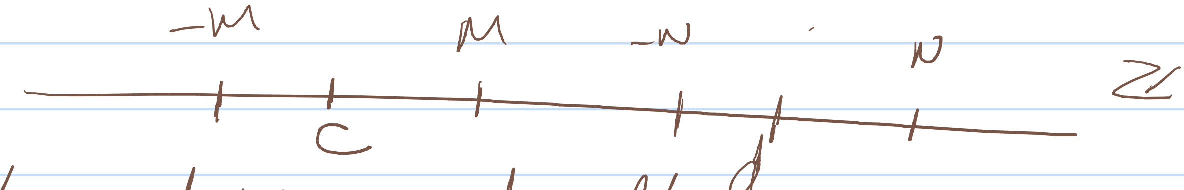
Então quando $b \neq 0$, temos:

$$\delta(a) = \delta(a) \cdot 1 \leq \delta(a) \cdot \delta(b) = \delta(ab)$$

Se $b \neq 0$, verificamos que a/b é um nº complexo que pode ser escrito na forma $c + di$, onde $c, d \in \mathbb{Q}$.
Se $c \in \mathbb{Q}$, esta está entre dois inteiros consecutivos, e d é similar

Então existem inteiros m e n sendo que: $|m-c| \le 1/2$ e $|n-d| \le 1/2$.

$b \neq 0$ e $a/b \in \mathbb{C} = (c+di) \in \mathbb{C}$ e $c, d \in \mathbb{Q}$



$|m-c| \le 1/2$ e $|n-d| \le 1/2$, $\frac{a}{b} = c+di$

$$\begin{aligned}
a &= b[c+di] \\
&= b[(c-m+m)+(d-n+n)i] \\
&= b[(m+ni)+((c-m)+(d-n)i)] \\
&= b[m+ni] + b[(c-m)+(d-n)i] \\
&= bq + r
\end{aligned}$$

Onde $q = m+ni \in \mathbb{Z}[i]$ e $r = b[(c-m)+(d-n)i]$
Portanto $r = a-bq$ e $a, b, q \in \mathbb{Z}[i]$, com isso $r \in \mathbb{Z}[i]$.

Propriedade (ii):

$$\begin{aligned}
\delta(r) &= \delta(b).\delta[(c-m)+(d-n)i] \\
&= \delta(b)[(c-m)^2+(d-n)^2] \\
&\le \delta(b)[(1/2)^2+(1/2)^2] = \frac{1}{2}.\delta(b) < \delta(b)
\end{aligned}$$

É possível que um dado domínio de integralidade pode ser feito em um domínio Euclidiano em que mais de uma forma por definição de função δ diferentemente. Sempre que domínio Euclidiano nos exemplos precedidos são mencionados, pode-se assumir que a função δ está definida.

Em $F[x]$, as unidades são polinômios de grau 0, isto é, os polinômios que tem o mesmo grau como polinômio identidade 1_F.

Portanto, se k é uma constante (unidade em $F[x]$), então $f(x)$ e $k(f(x))$ tem o mesmo grau. Fatos análogos mantém em qualquer domínio Euclidiano.

Teorema 10.2: Temos R sendo um domínio e u um elemento diferente de 0 em R. Então segue as condições são equivalentes:

1) u é uma unidade
2) $\delta(u) = \delta(1_R)$
3) $\delta(c) = \delta(uc)$ $\forall$ $c \neq 0$ e $c \in R$

Maiores divisores comuns: Os inteiros são ordenados por "$\leq$" e polinômios em $F[x]$ particionadamente ordenados por seus graus. Assim feito é natural definir MDC nestes domínios em termos do tamanho ou grau. A mesma ideia é transportada para domínios euclidianos, onde "tamanho" é medido pela função δ.

Definição: Temos R sendo um domínio euclidiano e $a, b \in R$ $(a, b \neq 0)$. Um MDC de a e b é um elemento d sendo que:

i) $d | a$ e $d | b$
ii) se $c | a$ e $c | b$, então $\delta(c) \leq \delta(d)$

Qualquer 2 elementos de um domínio euclidiano R tem pelo menos um divisor comum, chamado 1_R.

Se $c|a$, dizemos que $a=ct$, então:

$$\gamma(c) \leq \gamma(ct) = \gamma(a)$$

Consequentemente, cada divisor comum c de a e b satisfaz: $\gamma(c) \leq \max\{\gamma(a), \gamma(b)\}$, isto implica que existe um divisor comum maior possível γ. Noutras palavras, MDC sempre existe!

Quando MDC foram definidos em $\mathbb{Z}$ e $F[x]$, uma condição extra foi incluída em cada caso:

i) O MDC de 2 inteiros é o divisor comum de maior valor absoluto
ii) O MDC de 2 polinômios é o divisor mônico de maior grau.

Estas condições extras garante o MDC em $\mathbb{Z}$ e $F[x]$ são únicos. Em um domínio euclidiano arbitrário não existem muitas condições extras e MDC não são únicos. Assim o procedimento definido é consistente, mas não é idêntico para o que era feito em $\mathbb{Z}$ e $F[x]$.

Exemplo 8: $\mathbb{Z}$ é um domínio Euclidiano com $\delta(a) = |a|$.

Pela definição, 2 é mdc de 10 e 18. Contudo, (-2) também satisfaz esta definição porque (-2) divide 10 e 18 e qualquer divisor de 10 e 18 também tem valor absoluto $\leq |-2|$.
Note que o mdc 2 e (-2) são associados em $\mathbb{Z}$.

Teorema 10.3: Temos R sendo um domínio Euclidiano e $a, b \in R$, com $a, b \neq 0$.

1) Se d é o mdc de a e b, então cada associação de d é também um mdc de a, b.

2) Qualquer 2 mdc de a e b são associativos

3) Se d é um mdc de a e b, então existe $u, v \in R$ sendo que $d = au + bv$.

Corolário 10.4: Temos R sendo um domínio euclidiano e $a, b \in R$, com $a, b \neq 0$. Então d é um mdc de a e b, se e somente se, d satisfaz estas condições:

i) $d \mid a$ e $d \mid b$
ii) se $c \mid a$ e $c \mid b \rightarrow c \mid d$

Fatoração única:

Elementos a e b de um domínio euclidiano são ditos ser relativamente primos, se um dos mdc é 1_R. Em qualquer domínio as unidades são associativas de 1_R. Assim pelo Teorema 10.3, a e b são relativamente primos, se e somente se, um dos seus mdc é uma unidade.

Teorema 10.5: Temos R sendo um domínio euclidiano e $a, b, c \in R$. Se $a|bc$ e a e b são relativamente primos, então $a|c$.

Corolário 10.6: Temos "p" sendo um elemento irredutível em um domínio euclidiano R.

1) Se $p|bc$, então $p|b$ ou $p|c$,

2) Se $p|a_1a_2\ldots a_n$, então p divide pelo menos um dos a_i.

Teorema 10.7: Temos R sendo um domínio euclidiano, cada elemento diferente de zero e não unidade de R é o produto de elementos irredutíveis, e esta fatoração é única para associação, isto é, se:

$$p_1p_2\ldots\ldots p_r = q_1q_2\ldots\ldots q_s$$

Com cada p_i e q_i irredutível, então $r = 1$ e, após reordenar e redistribuir se necessário:

p_i é uma associação de q_i para $i = 1, 2, \ldots, r$