Um domínio euclidiano é, em efeito, um domínio que possui analogia com a divisão euclidiana (algoritmo da divisão). Consequentemente, todas as provas usadas para inteiros e anéis polinomiais, agora vamos considerar domínios que pode não ter uma analogia da divisão algorítmica, mas tem outra propriedade aritmética importante de $\mathbb{Z}$, sendo uma fatoração única e mdc.

Definição: Um domínio ideal principal (PID) ou (DIP) é um domínio de integralidade em que cada ideal é principal.

O próximo teorema mostra, por exemplo, que $\mathbb{Z}$, $\mathbb{Q}[x]$ e $\mathbb{Z}[i]$ são todos domínios de ideais principais porque todos eles são domínios euclidianos.

Teorema 10.8: Cada domínio euclidiano é um domínio ideal principal.

O inverso do teorema 10.8 é falso, existem domínios ideal principal que não são domínios euclidianos. Assim a classe de domínios euclidianos está estritamente contida na classe de domínios de ideal principal.

Em nosso desenvolvimento dos inteiros, anéis de polinômios e domínios euclidianos, primeiro consideramos mdc e usamos eles para provar fatoração única. Apesar desta abordagem também ser usada com domínios de ideais principais, isto é tão fácil quanto prosseguir diretamente para a fatoração única.

Lema 10.9: Temos a e b sendo elementos de um domínio integral R. Então:

1) $(a) \subseteq (b)$, se e somente se $b|a$
2) $(a) = (b)$, se e somente se $b|a$ e $a|b$
3) $(a) \subsetneq (b)$, " " " " $b|a$ e b não está associado com a.

Fatoração em primos: $a_1 = p_1 p_2 \ldots\ldots p_k \ldots 1 \cdot 1 \ldots$

Olhamos o mesmo procedimento do ponto de vista de ideais, temos:

$a_2|a_1$, $a_3|a_2$, $a_4|a_3, \ldots\ldots, 1|a_k$, $1|1$, $1|1$ e segue.

Pela Lema 10.9, este processo de fatoração segue para uma cadeia de ideais:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots\ldots \subseteq (a_k) \subseteq (1) \subseteq 1 \subseteq \ldots\ldots$$

Assim todos os ideais são iguais após algum ponto. Isto sugere que fatoração como um produto de irredutíveis relacionado a cadeias de ideais principais, em que todos os ideais são iguais em algum ponto.

Definição: Um domínio de integralidade R satisfaz a condição de cadeias ascendentes sobre ideais principais fornecida sempre que $(a_1) \subseteq (a_2) \subseteq \ldots\ldots$, então existem inteiros positivos N sendo que $(a_i) = (a_N)$ para todo $i \geq N$.

Lema 10.10: Todo domínio de ideal principal R satisfaz a condição de cadeias ascendentes sobre ideais principais.

O lema 10.10 é a chave para mostrar que cada elemento não unidade diferente de zero é um Domínio ideal principal pode ser fatorado como um produto de irredutíveis. Esta fatoração é única.

Lema 10.11: Temos R sendo um domínio de ideal principal. Se "p" é irredutível em R e $p \mid bc$, então $p \mid b$ ou $p \mid c$.

Teorema 10.12: Temos R sendo um domínio ideal principal. Todo elemento não unidade e diferente de zero de R é o produto de elementos irredutíveis e esta fatoração é única até associados, isto é, se:

$p_1 p_2 \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s$

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

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

Exemplo 1: Temos $Q_Z[x]$ denota o conjunto de polinômios com coeficientes racionais e inteiros termos constantes.

Ex: x, $\frac{1}{2}x$ e 2 estão em $Q_Z[x]$, mas:

$x^2 + \frac{1}{2}$ e $\frac{1}{4}$ não estão em $Q_Z[x]$.

Verifique que $Q_Z[x]$ é um domínio de integralidade e que o polinômio constante 2 é irredutível em $Q_Z[x]$.

O elemento irredutível 2 é um fator de $x \in Q_Z[x]$ porque $x = 2 \cdot \left(\frac{1}{2}x\right)$.

Similarmente, 2 é um fator irredutível de $\frac{1}{2}x$, porque: $\frac{1}{2}x = 2 \cdot \left(\frac{1}{4}x\right)$, então:

$x = 2 \cdot 2 \cdot \left(\frac{1}{4}x\right)$. De fato, o processo de fatoração irredutível de 2 nunca termina porque:

$x = 2\left(\frac{1}{2}x\right) = 2 \cdot 2\left(\frac{1}{4}x\right) = 2 \cdot 2 \cdot 2\left(\frac{1}{8}x\right), \dots, = 2 \cdot 2 \dots 2 \dots$

$\left(\frac{1}{2^n}x\right)$

Domínio de Fatoração única:

Definição: Um domínio de integralidade R é um domínio de fatoração única fornecido para cada elemento não unidade e diferente de R é o produto de elementos irredutíveis, e esta fatoração é única até associados, isto é, se:

$$p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

Com cada p_i e q_j irredutível, então $r = s$ e, depois reordenar e reorganizar se necessário:

p_i é um associado de q_j p/ $j = 1, 2, \ldots, r$.

Exemplo 2: Cada Domínio ideal principal é um domínio de fatoração única. Em particular, o anel $\mathbb{Z}[i]$ de inteiros gaussianos é um Domínio de fatoração única.

Exemplo 3: Como notado no exemplo 1, $\mathbb{Q}_{\mathbb{Z}}[x]$ não é um domínio de fatoração única, porque o elemento x não tem fatoração como um produto de um número finito de irredutíveis.

Na seção 10.3, iremos mostrar que $\mathbb{Z}[\sqrt{-5}]$ falha para ser um domínio de fatoração única por uma razão diferente: cada elemento é um produto de irredutíveis, mas esta fatoração não é única.

Exemplo 4: Uma prova que o anel polinomial $\mathbb{Z}[x]$ é um domínio de fatoração única, é dado na seção 10.5.

Desde que $\mathbb{Z}[x]$ não é um domínio de ideal principal, temos que a classe de todos os domínios de fatoração única é estritamente maior do que a classe de todos os domínios de ideal principal.

Teorema 10.13: Se c e d são elementos diferentes de zero em um domínio de fatoração única R, então existe unidades u e v e irredutíveis $p_1, p_2, \dots, p_k$ nenhum dos quais são associados, sendo que:

$$c = u p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \quad e \quad d = v p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

Onde cada m_i e n_i é um inteiro não negativo. Além do mais:

$$c \mid d \longrightarrow m_i \leq n_i \quad \forall\, i = 1, 2, \dots, k$$

Corolário 10.14: Todo domínio de fatoração única satisfaz a condição de cadeias ascendentes sobre ideais principais.

Irredutíveis em um domínio de fatoração única tem a propriedade que usamos frequentemente em casos especiais de domínios euclidianos e domínio de ideal principal.

Teorema 10.15: Temos p sendo um elemento irredutível em um domínio de fatoração única R. Se $p | bc \rightarrow p | b$ e $p | c$.

Teorema 10.16: Um domínio de integralidade R é um domínio de fatoração única se e somente se:

1) R tem condição de cadeias de ascendência sobre ideais principais,

2) Sempre que p é irredutível em R e $p | cd$, então $p | c$ ou $p | d$.

Maximo divisor comum:

Definição: Temos $a_1, a_2, \ldots, a_n$ sendo elementos (não todos diferentes de zero) de um domínio de integralidade R. Um mdc de $a_1, a_2, \ldots, a_n$ é um elemento d de R sendo que:

i) d divide cada um dos a_i
ii) se $c \in R$ e c divide cada um dos a_i, então $c | d$.

Teorema 10.17: Temos d sendo um mdc de $a_1, a_2, \ldots, a_n$ em um domínio de integralidade R. Então:

1| Toda associação de d é também um mdc de $a_1, \ldots, a_n$

2| Qualquer 2 mdc de $a_1, \ldots, a_n$ são associados.

<u>Teorema 10.18</u>: Temos $a_1, a_2, \ldots, a_n$ (não todos zero) sendo elementos em um domínio de fatoração única R. Então $a_1, \ldots, a_n$ tem um mdc em R.

Em um domínio de fatoração única arbitrário, ele pode não ser possível escrever o mdc dos elementos a e b como uma combinação linear de a e b como foi em $\mathbb{Z}$ e $F[x]$.

<u>Exemplo</u>: 1 é um mdc dos polinômios x e 2 em um domínio de fatoração única $\mathbb{Z}[x]$, mas 1 não é uma combinação de x e 2 em $\mathbb{Z}[x]$.

Em um domínio de ideal principal, contudo o mdc de a e b pode sempre ser escrito como uma combinação linear de a e b.