Aneis quocientes foram desenvolvidos como uma generalização natural de aneis $\mathbb{Z}_p$ e $F[x]/p(x)$.

Quando "p" é primo e $p(x)$ irredutível, então $\mathbb{Z}_p$ e $\frac{F[x]}{(p(x))}$ são corpos.

Primos em $\mathbb{Z}$ e irredutíveis em $F[x]$ essensialmente tem a mesma função nas estruturas da classe de aneis quocientes.

Um inteiro diferente de zero "p" (outros além ± 1) é primo se e somente se "p" tem esta propriedade:

Sempre que $p|bc$, então $p|b$ ou $p|c$.
Dizer que $p|a$ significa que $\underline{a}$ é um multiplo de "p", isto é, $\underline{a}$ é um elemento de um ideal principal (p) de todos os multiplos de "p". Assim esta propriedade de primos pode ser representada em termos de ideais:

"Se $p \neq 0, \pm 1$, então "p" é primo se e somente se, sempre que $bc \in (p)$, então $b \in (p)$ ou $c \in (p)$."

A condição $p \neq \pm 1$ garante que 1 não é multiplo de "p", e então o ideal (p) não é todo $\mathbb{Z}$.

Ideal principal: é um ideal gerado por um elemento.

① Definição: Um ideal "P" em um anel comutativo R é dito ser primo se $P \neq R$ e sempre que $bc \in P$, então $b \in P$ ou $c \in P$.

Exemplo 1: O ideal principal (p) é primo em $\mathbb{Z}$ sempre que "p" é um primo inteiro. Por outro lado, o ideal $P = (6)$ não é um primo em $\mathbb{Z}$ porque $2.3 \in P$, mas $2 \notin P$ e $3 \notin P$.

Exemplo 2: O ideal zero em qualquer domínio de integralidade R é primo porque $ab = 0_R \rightarrow a = 0_R$ ou $b = 0_R$.

Domínio de integralidade: é um anel comutativo com identidade sem divisores de zero.

i) $\exists 1 \in D\ (1 \neq 0$ e $\forall x \in D (1.x = x.1 = x))$, elemento neutro

ii) $\forall x, y \in D\ (x.y = y.x)$, comutativo

iii) $\forall x, y \in D\ (x.y = 0 \rightarrow (x = 0$ ou $y = 0))$, não existe divisores de zero

Exemplo 3: Se F é um corpo e $p(x)$ é irredutível em $F[x]$, então o ideal principal $(p(x))$ é primo em $F[x]$.

Exemplo 4:

Temos I sendo o ideal de polinômios com termos pares constantes em $\mathbb{Z}[x]$.

Então I não é um principal e claramente $I \neq \mathbb{Z}[x]$.

Temos $f(x) = a_n x^n + \ldots + a_0$ e $g(x) = b_m x^m + \ldots + b_0$ sendo polinômios em $\mathbb{Z}[x]$ e sendo que $f(x) \cdot g(x) \in I$.

Então o termo constante de $f(x)g(x)$, chamamos $a_0 b_0$, deve ser sempre par. Desde que o produto de dois inteiros impares é impar. Concluímos que a_0 é par (isto é, $f(x) \in I$) ou b_0 é par (isto é, $g(x) \in I$).

Portanto I é um ideal primo.

(O ideal I no exemplo 4 é primo, e o anel quociente $\mathbb{Z}[x]/I$ é um corpo. Similarmente, $\mathbb{Z}/(p) = \mathbb{Z}_p$ é um corpo quando "p" é primo. Contudo o próximo exemplo mostra que R/p pode não ser sempre um corpo quando "p" é primo.

Exemplo 5: O ideal principal (x) no anel $\mathbb{Z}[x]$ consiste de polinômios que são multiplos de x, isto é, polinômios com zero termos constantes.

Então, $(x) \neq \mathbb{Z}[x]$. Se $f(x) = a_n x^n + \dots + a_0$ e $g(x) = b_m x^m + \dots + b_0$ e $f(x)g(x) \in I$, então o termo constante de $f(x) \cdot g(x)$, chamamos ser 0.

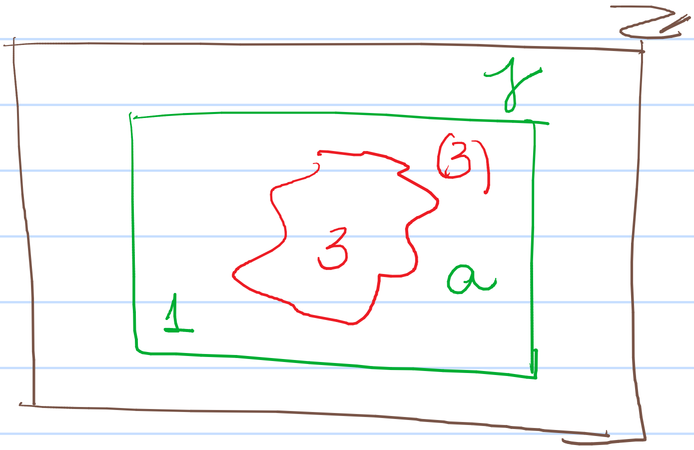
Isto pode acontecer se e somente se $a_0 = 0$ ou $b_0 = 0$, isto é, somente se $f(x) \in (x)$ ou $g(x) \in (x)$.

Portanto, (x) é um primo ideal. Contudo, o exemplo 7 da seção 6.2 mostra que o anel quociente $\frac{\mathbb{Z}[x]}{(x)}$ é isomorfo para $\mathbb{Z}$.
Portanto, $\frac{\mathbb{Z}[x]}{(x)}$ é um domínio de integralidade mas não é um corpo.

<u>Teorema 6.14</u>: Temos "P" sendo um ideal em um anel comutativo R com identidade. Então "P" é um ideal primo, se e somente se, o anel quociente $R/_P$ é um domínio de integridade.

<u>Exemplo 6</u>: Considere o ideal (3) em $\mathbb{Z}$, sabemos que $\mathbb{Z}/_{(3)} = \mathbb{Z}_3$ é um corpo.
Agora considere o ideal (3), suponha J é um ideal sendo que $(3) \subseteq J \subseteq \mathbb{Z}$. Se $J \neq (3)$, então existe $a \in J$ e $a \notin (3)$.
Em particular, $3 \nmid a$ então 3 e a são relativamente primos.
Então, existem inteiros u e v sendo que $3u + av = 1$. Desde que 3 e a estão no ideal J.

Segue que $1 \in J$, portanto $J = \mathbb{Z}$ e então não existem ideais estritos entre (3) e $\mathbb{Z}$.

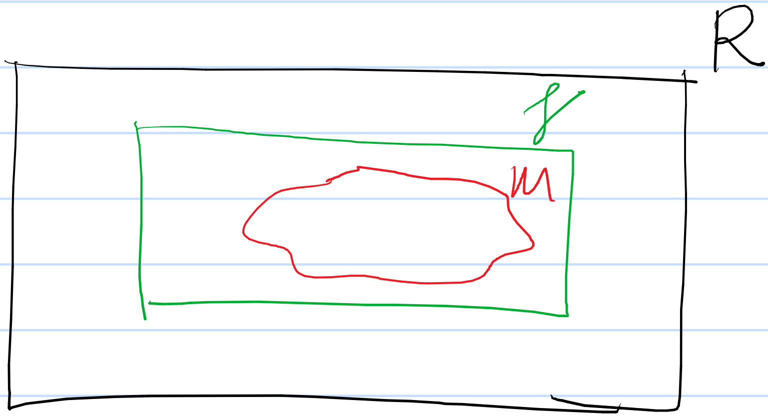


$3 \nmid a$
$mdc(3, a) = 1$

logo $J = \mathbb{Z}$

<u>Exemplo 7</u>: O anel quociente $\frac{\mathbb{Z}[x]}{(x)}$ não é um corpo (exemplo 5).
Além do mais, o ideal I de polinômios com termos constantes pares encontra-se estritamente entre (x) e $\mathbb{Z}[x]$, isto é,
$(x) \subsetneq I \subsetneq \mathbb{Z}[x]$.

<u>Definição</u>: Um ideal M em um anel R é dito ser maximal se $M \neq R$ e sempre que J é um ideal sendo que $M \subseteq J \subseteq R$, então $M = J$ ou $J = R$.



Teorema 6.15: Temos M sendo um ideal em um anel comutativo R com identidade. Então M é um maximal ideal se e somente se o anel quociente R/M é um corpo.

Corolário 6.16: Em um anel comutativo R com identidade, cada ideal maximal é primo.

Exemplo 8: O ideal I de polinômios com termos constantes pares em $\mathbb{Z}[x]$ é maximal porque $\frac{\mathbb{Z}[x]}{I}$ é um corpo.

Exemplo 9: Temos $\mathcal{F}$ sendo o anel de funções de R para R, e temos I sendo o ideal de todas funções g, sendo que $g(2)=0$.

No exemplo 8 da seção 6.2, vimos que $\mathcal{F}/I$ é um corpo isomorfo para R. Portanto, I é um ideal maximal em $\mathcal{F}$.