1| Mostre que o mapa $\theta : R[x] \to R$ que cada polinômio $f(x)$ para o termo constante é um homomorfismo sobrejetivo.

Mapa $\theta : R[x] \to R$, onde $R[x]$ é um polinômio em R.

$R[x] : f(x) \longrightarrow x$

polinômio   Constante - $x \in \mathbb{R}$

$$f(x_1) \longrightarrow x_1$$
$$\vdots \qquad\qquad \vdots$$
$$f(x_N) \longrightarrow x_N$$

Definição de Homomorfismo: Sobrejetivo ou epimorfismo: Se f for sobrejetivo, ou seja, quando $Im(f) = B$.

$$f : A \to B = Im(f)$$

1º| Determinamos o núcleo:

i) $N(f)$. Seja $x \in N(f) \to f(x) = 0 \leftarrow 0$ é um polinômio nulo e $f(0) = 0$. Então $N(f) \neq \phi$ e $N(f) = 0$.

ii) $Im(f)$. Seja $f(x) \in$ a $R[x]$, então $f(x_i)$ com $i = 1, \ldots, N$, temos que:

$$f(x_i) \longrightarrow x_i$$

Então $Im(f) = x_i$ onde $i = 0, 1, \ldots, N$ e $Im(f) = B$, todos os elementos da imagem.

2) Mostre que cada imagem homomórfica de um espaço F é cada isomorfismo para F para ele mesmo ou para anel zero.

Definição de Isomorfismo, seja $f: A \to B$ um homomorfismo de anéis, a função:

$$\varphi: \frac{A}{N(f)} \to Im(f), \text{ dada por } \varphi(\bar{a}) = f(a)$$

É um isomorfismo de anéis, ou seja, $\frac{A}{N(f)}$ é isomorfo a $Im(f)$.

→ Chamamos f de um isomorfismo se f for sobrejetivo e injetivo.

Prova: Primeiro temos que provar que somente ideais em um espaço F são $\{0_F\}$ e o próprio F. (ideais triviais)

i) Temos I, sendo um ideal em um espaço F, se $I \neq 0_F$, então existe algum elemento diferente de zero, $c \in F$ que pertence a I.

① Desde que F é um espaço e $c \neq 0_F$, c^{-1} existe. Assim I é um ideal, e então: $1 = c\,c^{-1} \in I$. Pela propriedade, temos novamente se $a \in F$, então $a = 1a \in I$. Logo $I = F$.

Homomorfismo

Agora temos R sendo um anel e $\phi: F \to R$, S ser a imagem de ϕ. Então S é um subanel de R, e podemos pensar que ϕ é sobrejetiva:

Mapa: $F \to S$

O núcleo K de ϕ é um ideal em F pelo Teorema . Pelo que podemos provar, cada $K = (0_F)$ ou $K = F$.

Portanto, temos o primeiro isomorfismo. $F/(0_F) \cong S$ ou $F/F \cong S$. Neste caso, $S \cong F$.

Em segundo caso, $S \cong F/S$, mas note que $[a] = [b]$ em F/F se e somente se:

$$a \equiv b \pmod F \rightarrow (a-b) \in F$$

Mas isto é verdade para cada 2 elementos a, b em F. Então F/F consiste de uma classe de congruência simples. Assim, F/F é um anel com somente um elemento. O único anel com um elemento é o anel zero.

---

3) Se F é um conjunto, R um anel diferente de zero, e $f: F \to R$ um homomorfismo sobrejetivo, prove que f é um isomorfismo.

Temos $f: F \to R$ sendo um homomorfismo sobrejetivo de um conjunto F para um anel não-trivial.

Supomos que existe $a \in F$, $a \neq 0_F$ sendo que $f(a) = 0_R$, então, desde que F é um conjunto

$f(a^{-1}) = f(a)^{-1} = 0^{-1}$

Como 0^{-1} é um anel zero, temos a possibilidade que $f: F \rightarrow R$ é um homomorfismo trivial $x \rightarrow 0$ para todo $x \in F$. Temos a sobrejetividade.

Outra alternativa, poderia ser o fato que somente ideais de conjunto triviais são $\{0\}$ e o próprio conjunto.

Se temos $a \in I$ e $a \neq 0$, então $1 \in I$ dis de que a^{-1} exista e $a.a^{-1} = 1 \in I$.
Assim podemos provar que núcleos de aneis homomorfilos são ideais, isto significa que homomorfismos fora do conjunto são os triviais ou injetivos.

4) Temos $[a]_N$ denota a classe de congruência de inteiros a modulo N.

a) Mostre que o mapa $f: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$ que envia $[a]_{12}$ para $[a]_4$ esta bem definido, homomorfismo sobrejetivo.

Epimorfismo: se f for sobrejetivo, ou seja, quando $Im(f) = B$. Dado $f: A \rightarrow B$ um homomorfismo de aneis.

$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$f: \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_4$

Determinamos o $Nuc(f)$.

Dado $x \in \mathbb{Z}_{12}$, com $x \equiv 0 (mod 12)$, temos que:

$x-12 \equiv 0 \rightarrow x-12 \equiv k, k | 12$.

Temos que $k|12$ possui resto zero. E temos que:

$$x \equiv 0 \ (mod\ 4)$$

Então temos que $\{0, 4, 8\} \in \mathbb{Z}_{12}$ é igual a zero em $\mathbb{Z}_4$. Portanto temos uma sobrejetividade.

$0 \equiv 0 \ (mod\ 4)$ *
$1 \equiv 1 \ (mod\ 4)$
$2 \equiv 2 \ (mod\ 4)$
$3 \equiv 3 \ (mod\ 4)$
$4 \equiv 0 \ (mod\ 4)$ *
$5 \equiv 1 \ (mod\ 4)$
$6 \equiv 2 \ (mod\ 4)$
$7 \equiv 3 \ (mod\ 4)$
$8 \equiv 0 \ (mod\ 4)$ *
$9 \equiv 1 \ (mod\ 4)$
$10 \equiv 2 \ (mod\ 4)$
$11 \equiv 3 \ (mod\ 4)$

Então $f(0)$, $f(4)$ e $f(8)$ são zeros na imagem.

O conjunto imagem é formado por:
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$ sendo que $\{0, 2\}$ possui imagem zero e $\{1, 3\}$ imagens diferentes de zero.

Temos um caso de Epimorfismo. Onde $Im f = B$. onde $f: A \rightarrow B$.

b) Nucleo de $f: \{0, 2\}$.

5) Temos I sendo um ideal em um domínio integral R. Isto é verdade que R/I é também domínio integral?

Definição de domínio integral: Temos um dado R sendo um anel comutativo. Um elemento a em R é chamado divisor zero se existe $b \neq 0$ em R sendo que $ab = 0$. Se R contém divisores diferente de zero, então R é chamado um domínio integral.

O anel quociente R/I de um domínio integral não é necessariamente um domínio integral. Considere, por exemplo, o anel de inteiros $\mathbb{Z}$ e ideal $I = 4\mathbb{Z}$. Note que $\mathbb{Z}$ é um domínio integral.

Podemos afirmar que o anel quociente $\mathbb{Z}/4\mathbb{Z}$ não é um domínio integral. De fato, o elemento $(2+4\mathbb{Z})$ é um elemento diferente de zero em $\mathbb{Z}/4\mathbb{Z}$. Temos que:

$$(2+4\mathbb{Z}).(2+4\mathbb{Z}) = 4+8\mathbb{Z}+8\mathbb{Z}+16\mathbb{Z} =$$
$$4+16\mathbb{Z}+16\mathbb{Z} = 4+32\mathbb{Z} = 0+\mathbb{Z}$$

Assim é um zero em $\mathbb{Z}/4\mathbb{Z}$.

Isto implica que $2+4\mathbb{Z}$ é um divisor de zero, e assim $\mathbb{Z}/4\mathbb{Z}$ não é um domínio integral.

Temos que o quociente R/I é um domínio integral, se e somente se, I é um primo ideal de R. No exemplo, o ideal $I = 4\mathbb{Z}$ é não é um ideal primo de $\mathbb{Z}$.

Em um anel A, um divisor de zero é um elemento diferente de zero que multiplicando por um outro elemento também diferente de zero, gera o zero.

Todos os números são divisores de zero, exceto o próprio zero. A definição de divisor é um número que divide outro número cujo resultado da divisão é um número inteiro.

① Domínio de integridade: é um anel comutativo com identidade sem divisores de zero.

Ideal Primo: é um subconjunto de um anel que tem várias propriedades em comum com as de um número primo do anel de inteiros. Os ideais primos para os inteiros são os conjuntos que contêm todos os múltiplos de um número primo dado, juntamente com o ideal nulo.

7) Se R é um anel, mostre que $R/(0_R) = R$.

Por definição de anéis quociente, os elementos de $R/(0_R)$ são da forma:

$$a + (0_R) = \{a\}$$

Isto é, são conjuntos consistindo somente por elementos $a \in R$. Então a função:

$f: R \to R/(0_R)$ por $f(a) = a + (0_R) = \{a\}$

Temos um isomorfismo. Assim:
$a \to a + (0_R)$ é o isomorfismo requerido de R para $R/\{0_R\}$.

Teorema: seja $f: A \to B$ um homomorfismo de anéis; a função $\varphi: \frac{A}{N(f)} \to Im(f)$, dada por $\varphi(\bar{a}) = f(a)$ é um isomorfismo de anéis, ou seja, $\frac{A}{N(f)}$ é isomorfo a $Im(f)$.

$$\begin{tikzcd} A \arrow[r] \arrow[d, dash] & B \\ A/N(f) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

4

8) Temos R e S dois anéis. Mostre que:
$\pi: R \times S \to R$, dado por $\pi(r,s) = r$ é um homomorfismo sobrejetivo cujo núcleo é isomorfo para S.

Temos que R, S são anéis, logo o produto cartesiano deles também é: $(R \times S)$ é um anel. Então dado:

$\pi: R \times S \to R$, $\pi(r,s) = r$, onde:
$(r,s) \in R \times S \to r \in R$

i) $\pi(R\times S) \to R$ é um homomorfismo sobrejetivo.

Seja $(r_1, s_1) \in R\times S$ logo $r_1 \in R$ e $s_1 \in S$, como

$\pi(r_1, s_1) \longrightarrow r_1$ temos que $\pi(s_1) = 0$. Ou seja $s_1 \in Nuc(f)$ e sua imagem é 0.
Portanto com R, S são aneis, $R\times S$ também e temos um epimorfismo de $R\times S$ para R.

ii) Se o núcleo de $R\times S$ é isomorfo a S, então todo elemento possui imagem 0.

Dada $\pi(r_1, s_1) = r \to (r\times 0) \to \pi(r_1) = r$ e $\pi(s_1) = 0$. Logo $s_1 \in$ Nucleo e S é o Nucleo de $R\times S$.

---

9) $R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\}$ é um anel com identidade.

Anel com identidade: $\exists 1 \in A$ tal que $a.1 = a$, $a = a$ $\forall a \in A$, dizemos que $(A, +, \cdot)$ é um anel com identidade e neste caso é 1 a identidade.

Um anel $(R, +, \cdot)$, onde a operação $\cdot$ é comutativa é dito ser um anel comutativo. Um $(R, +, \cdot)$ onde $\cdot$ tem elemento neutro é dito ser um anel com elemento identidade ou simplesmente, um anel com 1. Tal elemento neutro será indicado por 1 ou 1_R.

Um anel com identidade, ou anel com unidade é um anel com elemento neutro da multiplicação, denominado 1. Esse elemento sempre é único.

Proposição: Se um anel A possui unidade, então ela é única.

Seja $1, 1' \in A$ identidades distintas, ou seja, $\forall x \in A$ temos $1 \cdot x = x$ e $1' \cdot x = x$. Segue que $1 \cdot 1' = 1'$ mas $1'$ também é unidade, então $1 \cdot 1' = 1$ portanto $1 = 1'$.

a) Mostre que o mapa $f: R \to \mathbb{Z}$ dado por $f\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = a$ é um homomorfismo sobrejetivo.

Temos que: $f\begin{pmatrix} a_i & 0 \\ b & c \end{pmatrix} = a_i$ onde $f: R \to \mathbb{Z}$

Um homomorfismo subjetivo é dado por $Im(f) = B$ onde $f: A \to B$

Se a_i onde $i = 0, \ldots, N$ e temos que $a_0 = 0$, logo $f\begin{pmatrix} a_0 & 0 \\ b & c \end{pmatrix} = 0$ então $a_0 \in Nuc(f)$.

Assim a imagem de $\mathbb{Z}$ é igual a $\mathbb{Z}$ e portanto um epimorfismo. Sendo que para a_i com $i \neq 0$ as imagens são diferentes de zero.

b) O nucleo é dado por $\begin{pmatrix} a_0 & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix}$

11) $\mathbb{Z}[\sqrt{2}]$ é um anel, temos que:

$f: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ sendo uma função definida por:

$$f(a+b\sqrt{2}) = a - b\sqrt{2}$$

a) Mostre que f é um homomorfismo sobrejetivo de anéis.

Temos $f: \mathbb{Z}(\sqrt{2}) \to \mathbb{Z}(\sqrt{2})$, definida por:

$f(a+b\sqrt{2}) = a - b\sqrt{2}$, $\forall a+b\sqrt{2} \in \mathbb{Z}(\sqrt{2})$ é um homomorfismo.

Dados dois elementos de $\mathbb{Z}(\sqrt{2})$ no domínio, sendo $(a+b\sqrt{2})$ e $(c+d\sqrt{2})$, então:

- $f((a+b\sqrt{2}) + (c+d\sqrt{2})) = f(a+c+(b+d)\sqrt{2}) = a+c-(b+d)\sqrt{2} = (a-b\sqrt{2}) + (c-d\sqrt{2}) = f(a+b\sqrt{2}) + f(c+d\sqrt{2})$

- $f((a+b\sqrt{2}).(c+d\sqrt{2})) = f(ac+2bd+(ad+bc)\sqrt{2}) = ac+2bd-(ad+bc)\sqrt{2} = (a-b\sqrt{2}).(c-d\sqrt{2}) = f(a+b\sqrt{2}).f(c+d\sqrt{2})$

Temos que é um homomorfismo, tomamos agora o $nuc(f)$. Onde:

$f(a+b\sqrt{2}) = 0$, se a, b são iguais a zero.

$f(0+0\sqrt{2}) = 0$ portanto o $nuc(f) \neq \phi$ e $nuc(f) = \{1\}$.

Agora tomando $a - b\sqrt{2} = 0$

$$a = b\sqrt{2}$$

Então o $Nuc(f) = \{1\}$ e $Im(f) = \mathbb{Z}\sqrt{2}$, temos um caso de epimorfismo.

b) Teorema 6.11: Temos $f: R \to S$ sendo um homomorfismo de aneis com nucleo K. Então $K = \{0_R\}$, se e somente se, f é injetivo.

Mostre que f é também injetivo e assim é um isomorfismo. (Você deve assumir que $\sqrt{2}$ é irracional).

Temos que o $Nuc(f) = \{1\}$ e o elemento e o: $a, b = 0 \to (0 + 0\sqrt{2})$. Devemos mostrar que f é injetivo, com isso assumimos que a, b, c e $d \in \mathbb{Z}\sqrt{2}$ e:

$$f(a+b\sqrt{2}) = f(c+d\sqrt{2})$$

Isto porque f é um isomorfismo, então:

$$f(a+b\sqrt{2}) = f(c+d\sqrt{2})$$
$$a - b\sqrt{2} = c - d\sqrt{2}$$
$$a - c = -d\sqrt{2} + b\sqrt{2}$$
$$a - c = \sqrt{2}(b-d)$$
$$\frac{(a-c)}{(b-d)} = \sqrt{2}$$

Mas $\sqrt{2} \in \mathbb{R}/\mathbb{Q}$ logo não pode ser fatorado em números primos. Com isso temos que

$$f(a+b\sqrt{2}) \neq f(c+d\sqrt{2})$$

E portanto é injetivo e consequentemente é um isomorfismo.

12) Temos I sendo um ideal em um anel R não comutativo, sendo que $ab - ba \in I$ para todo $a, b \in R$. Prove que $R/_I$ é comutativo.

Temos que $R/_I$ é um anel quociente e os elementos são todos os conjuntos laterais gerados pela partição I de R. Assim,

$R/_I = \{r + I \mid r \in R\}$ desde que todos os conjuntos laterais são da forma $r + I$. Para mostrar que um anel é comutativo, deve-se garantir que para qualquer r, s no anel $rs = sr$.

No anel quociente, a multiplicação está definida como:

$$
\begin{aligned}
(r+I).(s+I) &= rs + rI + sI + I^2 \\
&= rs + I(r+s) + I \\
&= r.s + r+s + I
\end{aligned}
$$

Tomamos os elementos $(r+I)$ e $(s+I)$, agora devemos mostrar:

$$
\begin{aligned}
(r+I)(s+I) &= (s+I)(r+I) \\
rs + r + s + I &= rs + r + s + I \\
rs + r + s - rs - r - s &= I - I
\end{aligned}
$$

Como I é um anel, $I - I$ é simplesmente I porque a adição é fechada. Assim, $R/_I$ é comutativa somente se, for $r, s \in R$ e $(rs - sr) \in R$.

Assim podemos afirmar que: se R é comutativo, $R/_I$ também é comutativo.

13) Temos I sendo um ideal em um anel R. Prove que cada elemento em $R/_I$ tem uma raiz quadrada, se e somente se, para cada $a \in R$, existe $b \in R$ sendo que $(a-b^2) \in I$

Temos que para cada elemento em $R/_I$, vale:

i) $(a+c)+I=(b+d)+I$
ii) $ac+I=bd+I$

Temos que $R/_I$, sendo o conjunto das classes de equivalência modulo I. Dado por:
$\bar{a}=a+I$

Temos que $(a-b^2) \in I \rightarrow b^2 \equiv a \pmod{I}$

Assim dados $a,b \in R$, cada elemento que pertence a $R/_I$ possui raiz quadrada. Assim

$R/_I = B = \{\bar{b}, b_1, \ldots\} \rightarrow b \equiv \sqrt{a} \pmod{I}$

$(b)^2 \equiv (\sqrt{a})^2 \pmod{I}$

$b^2 \equiv a \pmod{I}$

Então: $(a-b^2) \in I$

15) Temos I sendo um ideal em um anel comutativo R. Prove que R/I tem uma identidade, se e somente se, existe $e \in R$ sendo que $ea \to a \in I$ para cada $a \in R$.

Teorema 6.8: Temos I sendo um ideal em um anel R. Se $a+I = b+I$ e $c+I = d+I$ em R/I, então:

$$(a+c)+I = (b+d)+I \quad e \quad ac+I = bd+I$$

Teorema 6.9: Temos I sendo um ideal em um anel R. Então:

1) R/I é um anel, com adição e multiplicação de conjuntos laterais como definido previamente.

2) Se R é comutativo, então R/I é um anel comutativo

3) Se R tem uma identidade, então R/I também tem.

Pelo teorema 6.9 temos que como R é comutativo, então R/I também é. Se R tem identidade "e" então R/I também tem identidade.

$\exists e \in R$ tal que: $(e+I)(a+I) = a+I \ \forall a \in R$. Esta equação é equivalente a: $ea + I = a+I$, e isto é o mesmo que $(ea - a) \in R$.

14) Temos I sendo um ideal em um anel R. Prove que cada elemento em $R|I$ é uma solução de $x^2 = x$, se e somente se, for cada $a \in R$, $a^2 - a \in I$.

Se $a \in R$, então $a+I$ é uma solução de $x^2 = x$ em $R|I$ se, e somente se, $a+I = (a+I)^2 = a^2+I$.

Temos que $(a+I) \in R/I$, $(a+I)^2 = a^2 + 2aI + I^2$
$= a^2 + 2aI + I$

$(a+I)^2 = (a+I).(a+I)$, onde $(a+I) \in R/I$

Temos que o produto de dois elementos esta no anel. Então:
$$(a+I)^2 = a^2 + I$$

Assim I é um subanel e Ideal de R, $I \subseteq R$.
Como $a \in R$, então $a+I \in I$ sendo uma solução de $x^2 = x$ em R/I, se e somente se, $a+I = (a+I)^2 = a^2+I$

Isso ocorre se, e somente se, $a - a^2 \in R$.

6) A função $\varphi: \mathbb{R}[x] \to \mathbb{R}$ dada por $\varphi(f(x)) = f(2)$ é um homomorfismo de aneis pelo exercicio 24 da seção 4.4 (com $a=2$). Encontre o nucleo de φ.

Teorema 6.12: Temos I sendo um ideal em um anel R. Então o mapa: $\pi: R \to R/I$ dado por $\pi(r) = r + I$ é um homomorfismo sobrejetivo com núcleo I.

"O mapa π é chamado de homomorfismo natural de R para R/I."

Teorema 6.11: Temos $f: R \to S$ sendo um homomorfismo de aneis com núcleo K. Então $K = (0_R)$ se e somente se, f é injetiva.

Teorema 6.10: Temos $f: R \to S$ sendo um homomorfismo de aneis. Então o núcleo K de f é um ideal em um anel R.

Pelo teorema 6.10 temos que o núcleo de φ é um ideal em $\mathbb{R}[x]$, ou seja $Nuc(\varphi)$ é o conjunto dos elementos $f(x) \in \mathbb{R}[x]$. Tais que:

$f(2) = 0$, isto é 2 é a raiz dos polinômios de $f(x) \in \mathbb{R}[x]$.

Temos que $(x-2)$ é um fator de $f(x)$, com isto o $Nuc(\varphi)$ é o conjunto de polinômios que são múltiplos de $(x-2)$, ou seja, $Nuc(\varphi) = ((x-2))$, e o ideal é gerado por $(x-2)$, de acordo com o teorema 6.11!

10) a) Temos $f: R \to S$ sendo um homomorfismo sobrejetivo de anéis e temos I sendo um ideal em R.
Prove que $f(I)$ é um ideal em S, onde $f(I) = \{s \in S \mid s = f(a) \; \forall a \in I\}$.

Temos que I é um ideal em R, ou seja I é um subanel de R. $I \subseteq R$.

Pela definição de I temos que:

i) dado $s, t \in f(I) \longrightarrow s = f(a)$ e $t = f(b)$ para alguns $a, b \in I$. Então:

$s + t = f(a) + f(b) = f(a+b) \in f(I)$, pois é homomorfismo.

ii) Agora, note que sendo f sobrejetiva temos que para qualquer $u \in S$ existe $r \in R$ tal que $f(r) = u$.
Então, $us = f(r) . f(a) = f(ra) = f(ar)$ e $us \in f(I)$. Desta forma, temos que $su \in f(I)$.
E, portanto, $f(I)$ é um ideal.

b) Mostre pelo enunciado de (a) que pode ser falsa se f não é sobrejetiva.

Considere, por exemplo, a aplicação de inclusão:
$\varphi : \mathbb{R} \to \mathbb{C}$
A qual é um homomorfismo, temos que $\mathbb{R}$ é um ideal de $\mathbb{R}$, mas $\phi(\mathbb{R}) = \mathbb{R}$ não é ideal em $\mathbb{C}$.