A definição das operações no anel quociente A/I garante que a passagem de A a A/I preserva as operações do anel. Com efeito, a aplicação

$$\begin{array}{rcl} p : A & \to & A/I \\ a & \mapsto & a+I \end{array}$$

satisfaz, pela maneira como definimos as operações em A/I, as propriedades

$$p(a+b) = p(a) + p(b)$$

$$p(ab) = p(a)p(b),$$

para quaisquer $a, b \in A$.

HOMOMORFISMO DE ANÉIS
Sejam A e B dois anéis. Uma aplicação $f : A \to B$ diz-se um homomorfismo de anéis se, para quaisquer $a, b \in A$, $f(a+b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$.

Portanto, $p : A \to A/I$ é um homomorfismo, claramente sobrejectivo.

APLICAÇÃO: Critérios de divisibilidade para os inteiros

Vejamos outro exemplo de homomorfismo. Consideremos a aplicação $f_m : \mathbb{Z} \to \mathbb{Z}_m$ do anel $(\mathbb{Z}, +, \cdot)$ no anel $(\mathbb{Z}_m, \oplus_m, \otimes_m)$ que a cada inteiro a faz corresponder a mod m, isto é, o resto da divisão de a por m.

`[Verifique:` f_m `é um homomorfismo de anéis]`

Seja $a = a_n a_{n-1} \cdots a_1 a_0$ um inteiro com $n+1$ algarismos, escrito na base decimal. Como $a = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0$, então, usando o facto de que f_m é um homomorfismo de anéis, temos

$$f_m(a) = f_m(10^n) \otimes f_m(a_n) \oplus f_m(10^{n-1}) \otimes f_m(a_{n-1}) \oplus \cdots \oplus f_m(10) \otimes f_m(a_1) \oplus f_m(a_0)$$

No caso $m = 9$, como $f_9(10^n) = 1$, para qualquer natural n, obtemos

$$\begin{array}{rcl} f_9(a) & = & f_9(a_n) \oplus f_9(a_{n-1}) \oplus \cdots \oplus f_9(a_1) \oplus f_9(a_0) \\ & = & f_9(a_n + a_{n-1} + \cdots + a_1 + a_0), \end{array}$$

o que mostra que $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$. Portanto,

um inteiro é divisível por 9 sse a soma dos seus algarismos o é.

Como também $f_3(10^n) = 1$, o mesmo critério vale para o 3:

um inteiro é divisível por 3 sse a soma dos seus algarismos o é.

Temos agora uma receita para obter critérios úteis de divisibilidade por m, desde que $f_m(10^n)$ seja dado por uma expressão simples:

m=11:

$$f_{11}(10^n) = \begin{cases} 1 & \text{se } n \text{ é par} \\ -1 & \text{se } n \text{ é ímpar} \end{cases}$$

pelo que
$a_n a_{n-1} \cdots a_1 a_0$ *é divisível por 11 sse* $(-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots - a_1 + a_0$ *o é.*

m=2,5: nestes casos $f_m(10^n) = 0$ logo

$a_n a_{n-1} \cdots a_1 a_0$ *é divisível por 2 (resp. 5) sse* a_0 *o é.*

m=4:

$$f_4(10^n) = \begin{cases} 2 & \text{se } n = 1 \\ 0 & \text{se } n \geq 2 \end{cases}$$

logo

$a_n a_{n-1} \cdots a_1 a_0$ *é divisível por 4 sse* $2a_1 + a_0$ *o é.*

m=6: $f_6(10^n) = 4$ logo

$a_n a_{n-1} \cdots a_1 a_0$ *é divisível por 6 sse* $4a_n + 4a_{n-1} + \cdots + 4a_1 + a_0$ *o é.*

Estes exemplos ilustram bem a ideia de como um homomorfismo de anéis, bem escolhido, permite transferir um problema num determinado anel (no caso presente, saber se um inteiro é divisível por um determinado m) para outro anel, onde se torna mais fácil de resolver.

As funções também permitem transferir a estrutura de uma álgebra para um conjunto sem estrutura. Por exemplo, seja f a função do anel quociente $\mathbb{Z}/(p)$ no conjunto $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ que a cada $a + I$ faz corresponder $a \mod p$.

`[Verifique: f é uma bijecção]`

Então $\mathbb{Z}_p$ herda a estrutura de $\mathbb{Z}/(p)$ se definirmos em $\mathbb{Z}_p$ as operações

$$a \oplus b = f(a+I) \oplus f(b+I) := f((a+I)+(b+I)) = f(a+b+I) = (a+b) \mod p$$

(isto é, a adição módulo p) e

$$a \otimes b = f(a+I) \otimes f(b+I) := f((a+I)(b+I)) = f(ab+I) = ab \mod p$$

(a multiplicação módulo p). $\mathbb{Z}_p$ com esta estrutura herdada de $\mathbb{Z}/(p)$ é um corpo finito, chamado *corpo de Galois de ordem p* e habitualmente denotado por $\mathbb{F}_p$, e f é um homomorfismo bijectivo.

ISOMORFISMO DE ANÉIS

A um homomorfismo de anéis bijectivo chama-se *isomorfismo*.

Portanto f é um isomorfismo de corpos.
Por exemplo, por f, as tabelas das operações em $\mathbb{Z}/(5)$ são transformadas em

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

e $(\mathbb{Z}/(5), +, \cdot)$ é um corpo isomorfo a $(\mathbb{Z}, \oplus, \otimes)$.

CARACTERÍSTICA

Seja A um anel com identidade. Se existir algum $n \in \mathbb{N}$ tal que $n1 = 0$, ao menor deles chama-se *característica* de A e diz-se que A tem *característica positiva*. Se tal n não existe, diz-se que A tem característica 0.

(Uma vez que $n1 = 0$ sse $na = 0$ para qualquer $a \in A$, podemos dizer que a característica de A é igual ao menor natural n, caso exista algum, tal que $na = 0$ para todo o $a \in A$, ou, caso contrário, igual a 0; como esta condição alternativa não depende da identidade, toma-se para definição de característica no caso geral de um anel sem necessariamente identidade.)

`[Verifique:` $n1 = 0$ `sse` $na = 0$ `para qualquer` $a \in A$`]`

Proposição. *Todo o domínio de integridade com característica positiva tem característica prima.*

Demonstração. Seja D um domínio de integridade com característica positiva $n \geq 1$. Como $1 \neq 0$, $n \geq 2$. Se n não fosse um primo então $n = rs$ para algum par

de inteiros satisfazendo $1 < r, s < n$, o que implicaria $0 = n1 = (rs)1 = (r1)(s1)$. Como D não tem divisores de zero, seria $r1 = 0$ ou $s1 = 0$, um absurdo uma vez que n é o menor natural tal que $n1 = 0$. ∎

`[Observe: a comutatividade do anel não é relevante para esta prova]`

Corolário. *Todo o corpo finito tem característica prima.*

Demonstração. Seja C um corpo finito. Pela proposição anterior, bastará provarmos que a característica de C é positiva. Para isso, consideremos os elementos

$$1, 1+1, 1+1+1, \ldots$$

de C. Como C é finito, esta lista é finita, pelo que $r1 = s1$ para alguns naturais r, s tais que $1 \leq r < s$. Consequentemente, $(s-r)1 = 0$, o que mostra que a característica de C não é zero. ∎

Proposição. *Seja A um anel comutativo de característica prima p. Então, para quaisquer $a, b \in A$ e $n \in \mathbb{N}$:*

(a) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

(b) $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

Demonstração. (a) Provaremos só o caso $n = 1$ (uma simples indução sobre n completa a prova). Pela fórmula do Teorema Binomial, válido em qualquer anel comutativo,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

Como cada $\binom{p}{i}$, $0 < i < p$, que é um inteiro, é igual a

$$\frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i}$$

então $1 \cdot 2 \cdot \cdots \cdot i$ divide $p(p-1)\cdots(p-i+1)$. Mas p é primo e $i < p$ logo $1 \cdot 2 \cdot \cdots \cdot i$ divide $(p-1)\cdots(p-i+1)$. Assim, $\binom{p}{i} \equiv 0 \mod p$. Em conclusão, $(a+b)^p = a^p + b^p$.
(b) Basta observar que, pela alínea (a), $a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}$. ∎