APÊNDICE 1

Anel

Definição 1.1: Um conjunto não vazio R é dito um *anel associativo* se em R estão definidas duas operações, indicadas por + e $\cdot$, tais que para todos a, b e c em R:

1) $a + b$ está em R;
2) $a + b = b + a$;
3) $(a + b) + c = a + (b + c)$;
4) Existe um elemento neutro 0 em R tal que $a + 0 = a$ (para todo a em R);
5) Existe um elemento oposto $-a$ em R tal que $a + (-a) = 0$;
6) $a \cdot b$ está em R;
7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
8) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ (as duas leis distributivas).

Os axiomas de (1) a (5) afirmam simplesmente que R é um grupo abeliano com relação à operação +, que será denominada adição. Os axiomas (6) e (7) afirmam que R é fechado com relação a operação associativa $\cdot$, que chamaremos de multiplicação. O axioma (8) serve para relacionar as duas operações de R.

Sempre que falarmos de *anel,* fica entendido que estamos relacionando a um anel associativo.

Pode acontecer, ou não, que exista um elemento 1 em R tal que $a \cdot 1 = 1 \cdot a = a$ para todo a em R; se existir tal elemento, R é denominado *anel com elemento unidade*.

Se a multiplicação de R *é* tal que $a \cdot b = b \cdot a$ para todos a e b em R, então chamamos R de *anel comutativo*.

Definição 1.2: Se R é um anel comutativo, então $a \neq 0 \in R$ é dito um *divisor do zero* se existe um $b \in R$, $b \neq 0$, tal que $ab = 0$.

Definição 1.3: Um anel comutativo é um *anel de integridade* se não possui divisores do zero. Equivalentemente, *anel de integridade* é um anel comutativo tal que $ab = 0$ se, e somente se, $a = 0$ ou $b = 0$.

Definição 1.4: Um anel é dito *anel com divisão* se seus elementos não nulos formam um grupo com relação à multiplicação.

Exemplo 1.1: Seja $R = \mathbb{Z}$ com a adição e a multiplicação usuais. R é um anel comutativo com elemento unidade e sem divisores de zero.

Exemplo 1.2: Seja R o conjunto dos inteiros pares com as operações de adição e multiplicação usuais. R é um anel comutativo, sem divisores de zero e não possui elemento unidade.

Exemplo 1.3: Seja R o conjunto dos números racionais com as operações usuais de adição e multiplicação. R é um anel comutativo com elemento unidade. Além do mais, os elementos de R diferentes de 0, formam um grupo abeliano com relação à multiplicação. Um anel com esta última propriedade é denominado um *corpo*.

Exemplo 1.4: Seja R o conjunto dos inteiros mod 7 com a operação de adição e multiplicação mod 7. Isto é, os elementos de R são os símbolos $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$ onde:

1) $\overline{i} + \overline{j} = \overline{k}$ onde k é o resto da divisão de $i + j$ por 7, por exemplo, $\overline{4} + \overline{5} = \overline{2}$, pois $4 + 5 = 9$, o qual deixa resto 2 quando dividido por 7.

2) $\overline{i} \cdot \overline{j} = \overline{m}$, onde m é o resto da divisão de ij por 7, por exemplo, $\overline{5} \cdot \overline{3} = \overline{1}$, pois $5 \cdot 3 = 15$, o qual deixa resto 1 quando dividido por 7.

R é um anel comutativo com elemento unidade; e mais os elementos não nulos de R formam um grupo abeliano com relação à operação de multiplicação. R é um corpo. R é chamado corpo finito pois possui um número finito de elementos.

Exemplo 1.5: Seja C o conjunto de todos os símbolos (α, β), onde α e β são números reais. Definimos:

1) $(\alpha, \beta) = (\gamma, \delta)$ se, e somente se, $\alpha = \gamma$ e $\beta = \delta$.

Em C introduzimos uma adição, definida como segue.

Sejam $x = (\alpha, \beta)$ e $y = (\gamma, \delta)$ dois elementos em C. Definimos $x + y$ por:

$$x + y = (\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta).$$

Notemos que $x + y$ está novamente em C. Afirmamos que C é um grupo abeliano com relação a esta operação, onde $(0,0)$ é o elemento neutro para a adição, e $(-\alpha, -\beta)$ como o simétrico de (α, β) com relação à adição.

A fim de tornar C um anel, necessitamos ainda de uma multiplicação. Definimos: para $x = (\alpha, \beta)$, $y = (\gamma, \delta)$ em C.

2) $x \cdot y = (\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma)$.

Notemos que $x \cdot y = y \cdot x$. Além disso, $x \cdot (1,0) = (1,0) \cdot x = x$ de modo que $(1,0)$ é o elemento unidade de C.

Novamente, notamos que $x, y \in C$. Se $x = (\alpha, \beta) \neq (0,0)$, então pelo fato que α e β são reais e não, ambos, nulos, $\alpha^2 + \beta^2 \neq 0$. Assim, $y = \left(\frac{\alpha}{\alpha^2+\beta^2}, -\frac{\beta}{\alpha^2+\beta^2}\right)$ está em C.

Finalmente, vemos que $(\alpha, \beta) \cdot \left(\frac{\alpha}{\alpha^2+\beta^2}, -\frac{\beta}{\alpha^2+\beta^2}\right) = (1,0)$, ou seja, dado $x \in C$ existe $y \in C$ tal que $x \cdot y$ é o elemento unidade de C.

Assim notamos que C é um corpo. Se escrevermos, (α, β) como $\alpha + \beta i$ podemos verificar que C é outra forma de representação dos números complexos.

Proposição 1.1: Um anel de integridade finito é um corpo.

Corolário 1.1.1: Se p é um número primo, então $\mathbb{Z}_p$, o anel dos inteiros mod p, é um corpo.

Demonstração: Pela Proposição 1. basta provar que $\mathbb{Z}_p$ é um anel de integridade, pois ele possui apenas um número finito de elementos. Se $a, b \in J_p$ e $ab = 0$, então p divide, necessariamente, o inteiro ordinário ab, e assim, p, sendo um primo, divide necessariamente a ou b. Mas, então $a \equiv 0 \bmod p$ ou $b \equiv 0 \bmod p$, donde em $\mathbb{Z}_p$, um destes é 0. ■

Proposição 1.2: Se R é um anel, então, para todos $a, b \in R$,

1) $a0 = 0a = 0$.
2) $a(-b) = (-a)b = -(ab)$.
3) $(-a)(-b) = ab$.

Se, além disso, R possui um elemento unidade 1, então:

4) $(-1)a = -a$.
5) $(-1)(-1) = 1$.

Definição 1.6: Um subconjunto não vazio U de R é dito um *ideal* (bilateral) de R se:

1) U é um subgrupo de R com relação à adição.

2) Para todo $u \in U$ e $r \in R$, ur e ru estão em U.

Proposição 1.3: Qualquer polinômio em $F[x]$ pode ser escrito de uma única maneira como um produto de polinômios irredutíveis em $F[x]$.

Proposição 1.4: O ideal $A = (p(x))$ em $F[x]$ é um ideal maximal se, e somente se, $p(x)$ é irredutível sobre F.

A notação $(p(x)) = \{f(x) \cdot p(x);\ f(x) \in F[x]\}$ representa o ideal gerado por $p(x)$.

Definição 1.7: Um ideal $M \neq R$ num anel R é dito um *ideal maximal* de R se sempre que U for um ideal de R tal que $M \subset U \subset R$, então $R = U$ ou $M = U$.

Em outras palavras, um ideal M de R e um *ideal maximal* se é impossível encontrar um ideal próprio do anel que contenha M.

Teorema 1.1: Se R é um anel comutativo com elemento unidade e M é um ideal de R, então M é um ideal maximal de R se, e somente se, R/M é um corpo.

APÊNDICE 2

Homomorfismo de anéis

Definição 2.1: Uma aplicação ϕ do anel R no anel R' é dita um *homomorfismo* se
1) $\phi(a+b) = \phi(a) + \phi(b)$;
2) $\phi(ab) = \phi(a)\phi(b)$;
para todo $a, b \in R$.

Proposição 2.1: Se ϕ é um homomorfismo de R em R', então:
1) $\phi(0) = 0$;
2) $\phi(-a) = -\phi(a)$, para todo $a \in R$.

Definição 2.2: Um homomorfismo de R em R' é dito um *monomorfismo* se ele é uma aplicação injetora.

Definição 2.3: Dois anéis são ditos *isomorfos* se existe um monomorfismo sobrejetor entre eles.

Proposição 2.2: O homomorfismo ϕ de R em R' é um monomorfismo se, e somente se, $N(\phi) = (0)$, onde $N(\phi)$ é o núcleo de ϕ.

Teorema 2.1: Sejam R e R' anéis e ϕ um homomorfismo sobrejetor de R em R' com núcleo U. Então, R' é isomorfo a R/U. Além do mais, existe uma correspondência biunívoca entre o conjunto dos ideais de R' e o conjunto dos ideais de R que contêm U. Esta correspondência pode ser conseguida associando com um ideal W' de R' o ideal W de R definido por $W = \{x \in R \mid \phi(x) \in W'\}$. Com W assim definido R/W é isomorfo a R'/W'.