Álgebra Universal e Categorias

Carla Mendes

2024/2025

Departamento de Matemática

Elementos de álgebra universal

Elementos de álgebra universal

O desenvolvimento do estudo na área da matemática levou ao aparecimento de diversas estruturas algébricas, tais como grupos, anéis, reticulados, álgebras de Boole, etc. Tais estruturas, embora distintas, têm propriedades análogas, o que levou ao surgir de uma área da matemática, a Álgebra Universal, que tem por objetivo o estudo de propriedades que são comuns a todas estas estruturas.

Álgebras

Um dos conceitos básicos em álgebra universal, suficientemente abrangente para englobar muitas das estruturas algébricas que nos são familiares, é a noção de álgebra, a qual é definida como um conjunto não vazio equipado com uma família de operações.

Dados um conjunto A e um inteiro não negativo n, define-se $A^n = \{\emptyset\}$ se $n = 0$ e, para $n > 1$, A^n é o conjunto dos n-tuplos de elementos de A.

Definição

Sejam A um conjunto e $n \in \mathbb{N}_0$. Chama-se ***operação n-ária em A*** *a qualquer função f de A^n em A e ao inteiro n dá-se a designação de* ***aridade de f****. Uma* ***operação finitária*** *é uma operação n-ária, para algum $n \in \mathbb{N}_0$.*

Elementos de álgebra universal

A uma operação em A de aridade 0 dá-se a designação de ***operação nulária*** em A. Uma operação nulária em A é uma função $c : \{\emptyset\} \to A$, sendo esta função completamente determinada pelo elemento $c(\emptyset) \in A$ e usualmente identificada com esse elemento; por este motivo as operações nulárias são também designadas por ***constantes***.

Às operações de aridade 1, 2 e 3 é usual dar a designação de operações ***unárias***, ***binárias*** e ***ternárias***, respetivamente.

Definição

Dá-se a designação de ***tipo algébrico****, ou simplesmente* ***tipo****, a um par (O, τ), onde O é um conjunto e τ é uma função de O em $\mathbb{N}_0$. Cada elemento f de O é designado por* ***símbolo de operação*** *e $\tau(f)$ diz-se a sua* ***aridade****. O conjunto de todos os símbolos de O de aridade n é representado por O_n.*

Definição

Chama-se ***álgebra*** *a um par* $\mathcal{A} = (A; F)$ *onde* A *é um conjunto não vazio e* F *é uma família* $(f^{\mathcal{A}})_{f \in O}$ *de operações finitárias em* A*, indexada por um conjunto* O*.*

Ao conjunto A *dá-se a designação de* ***universo*** *ou* ***conjunto suporte de*** $\mathcal{A}$*, cada operação* $f^{\mathcal{A}}$ *é designada por* ***operação fundamental de*** $\mathcal{A}$ *ou* ***operação básica*** *de* $\mathcal{A}$ *e ao conjunto* O *dá-se a designação de* ***conjunto de símbolos operacionais de*** $\mathcal{A}$*.*

Uma álgebra $\mathcal{A}$ *diz-se uma* ***álgebra de tipo*** (O, τ) *se a família de operações de* $\mathcal{A}$ *é indexada por* O *e a cada símbolo operacional* $f \in O$ *está associada uma operação básica* $f^{\mathcal{A}}$ *de aridade* $\tau(f)$*.*

Elementos de álgebra universal

Ao longo do texto as álgebras são representadas por letras maiúsculas caligráficas, eventualmente com índices, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, ..., $\mathcal{A}_1$, $\mathcal{A}_2$, ..., e o conjunto suporte das álgebras é representado pelas letras maiúsculas respetivas, A, B, C, ..., A_1, A_2, ...

Uma álgebra $\mathcal{A} = (A; F)$ diz-se ***trivial*** se $|A| = 1$ e diz-se ***finita*** ou ***infinita*** caso o seu conjunto suporte A seja finito ou infinito, respetivamente.

Elementos de álgebra universal

Dada uma álgebra $\mathcal{A} = (A; (f^{\mathcal{A}})_{f \in O})$, usa-se a notação $f^{\mathcal{A}}$ para representar a operação fundamental de $\mathcal{A}$ indexada por $f \in O$; à operação $f^{\mathcal{A}}$ dá-se a designação de ***interpretação de*** f ***em*** $\mathcal{A}$. Caso o contexto seja claro pode escrever-se apenas f em vez de $f^{\mathcal{A}}$.

O conjunto de símbolos operacionais O de uma álgebra $\mathcal{A}$ pode ser finito ou infinito. Caso O seja finito, digamos $O = \{f_1, f_2, \ldots, f_n\}$, é usual escrever

$$\mathcal{A} = (A; {f_1}^{\mathcal{A}}, {f_2}^{\mathcal{A}}, \ldots, {f_n}^{\mathcal{A}}) \text{ ou apenas } \mathcal{A} = (A; f_1, f_2, \ldots, f_n)$$

e representa-se o tipo de $\mathcal{A}$ por

$$(O, n_{f_1}, n_{f_2}, \ldots, n_{f_n}) \text{ ou por } (n_{f_1}, n_{f_2}, \ldots, n_{f_n}),$$

onde n_{f_i}, $i \in \{1, \ldots, n\}$, representa a aridade da operação ${f_i}^{\mathcal{A}}$.

Elementos de álgebra universal

Uma álgebra $\mathcal{A}$ diz-se ***unária*** se $\mathcal{A}$ é uma álgebra de tipo (O, τ) onde $\tau(f) = 1$, para todo $f \in O$, ou seja, $\mathcal{A}$ é uma álgebra em que todas as operações fundamentais são unárias.

A uma álgebra $\mathcal{A}$ com uma única operação binária, ou seja, a uma álgebra de tipo $(\{f\}, \tau)$ onde $\tau(f) = 2$, dá-se a designação de ***grupóide***.

Exemplo

(i) Para qualquer conjunto não vazio A, $\mathcal{A} = (A; \emptyset)$ *é uma álgebra.*

(ii) Um ***semigrupo*** *é um grupóide* $\mathcal{S} = (S; \cdot)$ *tal que, para quaisquer* $x, y, z \in S$,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \tag{1.1}$$

ou seja, um semigrupo é uma álgebra definida por um conjunto não vazio munido de uma operação binária associativa.

Exemplo

*(iii) Um **monóide** é um semigrupo* $(M; \cdot)$ *com um elemento* $1_M \in M$ *tal que, para todo* $x \in M$,

$$x \cdot 1_M = x = 1_M \cdot x. \tag{1.2}$$

A um elemento 1_M *que satisfaça as condições anteriores dá-se a designação de elemento neutro ou identidade e é simples verificar que num dado semigrupo não existe mais do que um elemento destes. Assim, o elemento neutro pode ser interpretado como uma função constante e um monóide pode ser definido como uma álgebra* $\mathcal{M} = (M; \cdot, 1_M)$ *de tipo* $(2, 0)$ *que satisfaz as identidades (1.1) e (1.2).*

(iv) Um ***grupo*** pode ser descrito como um tipo especial de semigrupo, ou seja, como uma álgebra $(G; \cdot)$ de tipo (2) que satisfaz as identidades (1.1), (1.2) e tal que, para todo $x \in G$, existe $x^{-1} \in G$ tal que

$$x \cdot x^{-1} = 1_G = x^{-1} \cdot x. \tag{1.3}$$

Atendendo a que um grupo é um monóide, um grupo pode também ser definido como um monóide $(G; \cdot, 1_G)$ de tipo $(2, 0)$ que satisfaz a identidade (1.3).

Num grupo $(G;\cdot)$, para cada $x \in G$, existe um único elemento $x^{-1} \in G$ que satisfaz a identidade (1.3), pelo que faz sentido considerar uma operação unária que a cada elemento $x \in G$ associa o elemento x^{-1}. Por conseguinte, um grupo pode ser descrito como uma álgebra $\mathcal{G} = (G;\cdot,^{-1}, 1_G)$ de tipo $(2, 1, 0)$ que satisfaz (1.1), (1.2) e (1.3).

Um **grupo abeliano** é um grupo $\mathcal{G} = (G;\cdot,^{-1}, 1_G)$ tal que, para quaisquer $x, y \in G$, $x \cdot y = y \cdot x$.

(v) Um ***anel*** é uma álgebra $\mathcal{A} = (A; +, \cdot, -, 0_{\mathcal{A}})$ de tipo $(2, 2, 1, 0)$ tal que $(A; +, -, 0_{\mathcal{A}})$ é um grupo abeliano, $(A; \cdot)$ é um semigrupo e, para quaisquer $x, y, z \in A$,

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{e} \quad (y + z) \cdot x = y \cdot x + z \cdot x.$$

Um **anel com identidade** é uma álgebra $\mathcal{A} = (A; +, \cdot, -, 0_{\mathcal{A}}, 1_{\mathcal{A}})$ de tipo $(2, 2, 1, 0, 0)$ tal que $(A; +, \cdot, -, 0_{\mathcal{A}})$ é um anel e $(A; \cdot, 1_{\mathcal{A}})$ é um monóide.

(vi) Um ***semirreticulado*** é um semigrupo comutativo $\mathcal{S} = (S; \cdot)$ tal que, para todo $x \in S$,

$$x \cdot x = x.$$

(vii) Um ***reticulado*** é uma álgebra $\mathcal{R} = (R; \wedge, \vee)$ de tipo $(2,2)$ tal que, para quaisquer $x, y, z \in R$,

R1: $x \wedge y = y \wedge x$, R1$_d$: $x \vee y = y \vee x$;

R2: $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, R2$_d$: $x \vee (y \vee z) = (x \vee y) \vee z$;

R3: $x \wedge x = x$, R3$_d$: $x \vee x = x$;

R4: $x \wedge (x \vee y) = x$, R4$_d$: $x \vee (x \wedge y) = x$.

(viii) Um ***reticulado limitado*** é uma álgebra $\mathcal{R} = (R; \wedge, \vee, 0_{\mathcal{R}}, 1_{\mathcal{R}})$ de tipo $(2,2,0,0)$ tal que $(R; \wedge, \vee)$ é um reticulado e, para qualquer $x \in R$,

$$x \wedge 0_{\mathcal{R}} = 0_{\mathcal{R}} \quad \text{e} \quad x \vee 1_{\mathcal{R}} = 1_{\mathcal{R}}.$$

(ix) Um ***reticulado distributivo*** é um reticulado $\mathcal{R} = (R; \wedge, \vee)$ tal que, para quaisquer $x, y, z \in R$,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{e} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

(x) Uma ***álgebra de Boole*** é uma álgebra $\mathcal{B} = (B; \wedge, \vee, ', 0_{\mathcal{B}}, 1_{\mathcal{B}})$ de tipo $(2, 2, 1, 0, 0)$ tal que $(B; \wedge, \vee)$ é um reticulado distributivo e, para todo $x \in B$,

$$x \wedge 0_{\mathcal{B}} = 0_{\mathcal{B}}, \qquad x \vee 1_{\mathcal{B}} = 1_{\mathcal{B}},$$

$$x \wedge x' = 0_{\mathcal{B}}, \qquad x \vee x' = 1_{\mathcal{B}}.$$

A partir de uma determinada álgebra podem definir-se novas álgebras acrescentando operações fundamentais à álgebra dada.

Definição

*Sejam $\mathcal{A}$ e $\mathcal{B}$ álgebras de tipos (O_1, τ_1) e (O_2, τ_2), respetivamente. Diz-se que a álgebra $\mathcal{A}$ é uma **extensão** da álgebra $\mathcal{B}$ ou que $\mathcal{B}$ é um **reduto** da álgebra $\mathcal{A}$ se: $\mathcal{A}$ e $\mathcal{B}$ têm o mesmo universo, $O_2 \subseteq O_1$ e, para todo $f \in O_2$, $\tau_1(f) = \tau_2(f)$ e $f^{\mathcal{A}} = f^{\mathcal{B}}$.*

Exemplo

O semigrupo $(\mathbb{R}; +)$ é um reduto do anel $(\mathbb{R}; +, \cdot)$.

Subálgebras

Em certas situações, o estudo de uma álgebra pode ser simplificado recorrendo ao estudo de outras álgebras que estejam relacionadas com a álgebra dada. Por este motivo, é importante considerar processos que permitam construir novas álgebras a partir de uma determinada álgebra. Um desses processos corresponde à formação de subálgebras.

Definição

*Sejam A um conjunto, $n \in \mathbb{N}_0$, f uma operação n-ária em A e $X \subseteq A$. Diz-se que o **conjunto** X **é fechado para a operação** f se*

$$f(a_1, \ldots, a_n) \in X, \text{ para todo } (a_1, \ldots, a_n) \in X^n.$$

Observação: Se f é uma operação nulária num conjunto A, então um conjunto $X \subseteq A$ é fechado para a operação f se e só se $f \in X$. Por conseguinte, se $X = \emptyset$, o conjunto X não é fechado para qualquer operação nulária. Note-se, no entanto, que $X = \emptyset$ é fechado para toda toda a operação n-ária sempre que $n \geq 1$.

Definição

*Sejam $\mathcal{A} = (A; F)$ uma álgebra. Um subconjunto B de A diz-se um **subuniverso** de $\mathcal{A}$ se B é fechado para toda a operação de F. Representa-se por $\mathrm{Sub}\mathcal{A}$ o conjunto de todos os subuniversos de $\mathcal{A}$.*

Observação: O conjunto vazio é subuniverso de uma álgebra $\mathcal{A}$ se e só se $\mathcal{A}$ não tem operações nulárias.

Exemplo

(1) Os conjuntos $\{0\}$, $\{2n \mid n \in \mathbb{Z}\}$ *e* $\mathbb{Z}$ *são subuniversos do semigrupo* $(\mathbb{Z}; +)$ *e do anel* $(\mathbb{Z}; +, \cdot, -, 0)$.

(2) O conjunto $\{2n+1 \mid n \in \mathbb{Z}\}$ *não é subuniverso do semigrupo* $(\mathbb{Z}; +)$ *nem do anel* $(\mathbb{Z}; +, \cdot, -, 0)$.

(3) O conjunto $\emptyset$ *é um subuniverso do semigrupo* $(\mathbb{Z}; +)$, *mas não é subuniverso do anel* $(\mathbb{Z}; +, \cdot, -, 0)$.

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $\{S_i \mid i \in I\}$ *uma família não vazia de subuniversos de* $\mathcal{A}$. *Então* $\bigcap_{i \in I} S_i$ *é um subuniverso de* $\mathcal{A}$.

Demonstração.

Para cada $i \in I$, S_i é um subuniverso de $\mathcal{A}$, pelo que $S_i \subseteq A$. Assim, $\bigcap_{i \in I} S_i \subseteq A$.

Além disso, para qualquer operação n-ária $f^{\mathcal{A}}$ e para qualquer $(a_1, \ldots, a_n) \in \left(\bigcap_{i \in I} S_i\right)^n$, tem-se $f^{\mathcal{A}}(a_1, \ldots, a_n) \in S_i$, para cada $i \in I$, pois $(a_1, \ldots, a_n) \in (S_i)^n$ e cada um dos conjuntos S_i é um subuniverso de $\mathcal{A}$. Então $f^{\mathcal{A}}(a_1, \ldots, a_n) \in \bigcap_{i \in I} S_i$ e, portanto, $\bigcap_{i \in I} S_i$ é fechado para a operação $f^{\mathcal{A}}$. $\square$

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra,* $X \subseteq A$ *e*

$$S = \bigcap \{B \mid B \text{ é subuniverso de } \mathcal{A} \text{ e } X \subseteq B\}.$$

Então S *é um subuniverso de* $\mathcal{A}$ *e é o menor subuniverso de* $\mathcal{A}$ *que contém* X*.*

Demonstração.

Uma vez que A é um subuniverso de $\mathcal{A}$ e $X \subseteq A$, então a família

$$\{B \mid B \text{ é subuniverso de } \mathcal{A} \text{ e } X \subseteq B\}$$

é não vazia e do teorema anterior segue que S é um subniverso de $\mathcal{A}$. Da definição de S é imediato que $X \subseteq S$ e que S está contido em qualquer subuniverso de $\mathcal{A}$ que contenha X. $\square$

Definição

Sejam $\mathcal{A} = (A; F)$ *uma álgebra,* $X \subseteq A$ *e* S *um subuniverso de* $\mathcal{A}$*. Designa-se por* ***subuniverso de*** $\mathcal{A}$ ***gerado por*** X*, e representa-se por* $Sg^{\mathcal{A}}(X)$*, o menor subuniverso de* $\mathcal{A}$ *que contém* X*, i.e., o conjunto*

$$Sg^{\mathcal{A}}(X) = \bigcap \{B \mid B \text{ é subuniverso de } \mathcal{A} \text{ e } X \subseteq B\}.$$

Diz-se que S *é* ***finitamente gerado*** *se* $S = Sg^{\mathcal{A}}(X)$*, para algum conjunto finito* $X \subseteq A$*.*

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $X \subseteq A$. *Definem-se recursivamente*

$$\begin{array}{lcl} X_0 & = & X; \\ X_{i+1} & = & X_i \cup \{f^{\mathcal{A}}(x) \mid f^{\mathcal{A}} \text{ é operação } n\text{-ária em } \mathcal{A} \text{ e } x \in (X_i)^n, n \in \mathbb{N}_0\}. \end{array}$$

Então $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$.

Demonstração.

É imediato que $X \subseteq \bigcup_{i \in \mathbb{N}_0} X_i \subseteq A$.

Facilmente também se verifica que $\bigcup_{i \in \mathbb{N}_0} X_i$ é fechado para toda a operação de $\mathcal{A}$:

Se $f^{\mathcal{A}}$ é uma operação n-ária em $\mathcal{A}$ e $a_1, \ldots, a_n$ são elementos tais que $(a_1, \ldots, a_n) \in (\bigcup_{i \in \mathbb{N}_0} X_i)^n$, tem-se $(a_1, \ldots, a_n) \in (X_k)^n$, para algum $k \in \mathbb{N}_0$, donde $f^{\mathcal{A}}(a_1, \ldots, a_n) \in X_{k+1} \subseteq \bigcup_{i \in \mathbb{N}_0} X_i$.

Logo, $\bigcup_{i \in \mathbb{N}_0} X_i$ é um subuniverso de $\mathcal{A}$ e contém X.

Além disso, $\bigcup_{i \in \mathbb{N}_0} X_i$ é o menor subuniverso de $\mathcal{A}$ que contém X. De facto, se B é um subuniverso de $\mathcal{A}$ que contém X, mostra-se, por indução em i, que $X_i \subseteq B$, para todo $i \in \mathbb{N}_0$, e, por conseguinte, $\bigcup_{i \in \mathbb{N}_0} X_i \subseteq B$.

Assim, $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$. $\square$

Corolário

Sejam $\mathcal{A}$ *uma álgebra,* $X \subseteq A$ *e* $a \in Sg^{\mathcal{A}}(X)$*. Então* $a \in Sg^{\mathcal{A}}(Y)$*, para algum subconjunto finito* Y *de* X*.*

Demonstração.

Do teorema anterior sabe-se que $Sg^{\mathcal{A}}(X) = \bigcup_{i \in \mathbb{N}_0} X_i$, onde X_i são os conjuntos descritos nesse mesmo teorema. Por indução em i prova-se que se $a \in X_i$, então $a \in Sg^{\mathcal{A}}(Y)$, para algum subconjunto finito Y de X. $\square$

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $X, Y \subseteq A$. *Então*

(i) $X \subseteq Sg^{\mathcal{A}}(X)$.

(ii) $X \subseteq Y \Rightarrow Sg^{\mathcal{A}}(X) \subseteq Sg^{\mathcal{A}}(Y)$.

(iii) $Sg^{\mathcal{A}}(Sg^{\mathcal{A}}(X)) = Sg^{\mathcal{A}}(X)$.

(iv) $Sg^{\mathcal{A}}(X) = \bigcup\{Sg^{\mathcal{A}}(Z) \mid Z \text{ é subconjunto finito de } X\}$.

Observe que os subuniversos de uma álgebra $\mathcal{A}$ são exatamente os subconjuntos X de A para os quais se tem $X = Sg^{\mathcal{A}}(X)$.

Teorema

Sejam $\mathcal{A}$ uma álgebra. Então $(\mathrm{Sub}\mathcal{A}, \subseteq)$ *é um reticulado algébrico, tendo-se, para quaisquer $B, C \in \mathrm{Sub}\mathcal{A}$,*

$$B \wedge C = B \cap C, \;\; B \vee C = Sg^{\mathcal{A}}(B \cup C), \; \forall B, C \in \mathrm{Sub}\mathcal{A}.$$

Os elementos compactos de $(\mathrm{Sub}\mathcal{A}, \subseteq)$ *são os subuniversos de $\mathcal{A}$ finitamente gerados.*

Definição

Sejam $\mathcal{A} = (A; F)$ *e* $\mathcal{B} = (B; G)$ *álgebras do mesmo tipo* (O, τ). *Diz-se que* $\mathcal{B}$ *é uma* ***subálgebra*** *de* $\mathcal{A}$, *e escreve-se* $\mathcal{B} \leq \mathcal{A}$, *se* B *é um subuniverso de* $\mathcal{A}$ *e, para todo* $n \in \tau(O)$ *e todo o símbolo de operação* $f \in O_n$,

$$f^{\mathcal{B}}(b_1, \ldots, b_n) = f^{\mathcal{A}}(b_1, \ldots, b_n),$$

para qualquer $(b_1, \ldots, b_n) \in B^n$.

Observação: Se $\mathcal{B} = (B; G)$ é subálgebra de uma álgebra $\mathcal{A} = (A; F)$, então B é um subuniverso de $\mathcal{A}$. No entanto, um subuniverso de $\mathcal{A}$ não é necessariamente o universo de uma subálgebra de $\mathcal{A}$. Observe-se que o conjunto vazio pode ser subuniverso de uma álgebra $\mathcal{A}$, mas não é universo de qualquer subálgebra de $\mathcal{A}$.

Exemplo

1) O anel $(\mathbb{R}; +, \cdot, -, 0)$ *é uma subálgebra do anel* $(\mathbb{C}; +, \cdot, -, 0)$.

2) Se $(G; \cdot)$ *é grupo, as suas subálgebras são os subsemigrupos de* G.

3) Se $(G; \cdot, ^{-1}, 1)$ *é grupo, as suas subálgebras são os subgrupos de* G.

Definição

Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X \subseteq A$ tal que $X \neq \emptyset$. Chama--se ***subálgebra de $\mathcal{A}$ gerada por*** *X, e representa-se por $\mathcal{S}g^{\mathcal{A}}(X)$, a subálgebra de $\mathcal{A}$ cujo universo é $Sg^{\mathcal{A}}(X)$.*

Se na álgebra $\mathcal{A}$ há, pelo menos, uma operação nulária, define-se a ***subálgebra de $\mathcal{A}$ gerada por*** *$\emptyset$ como sendo a subálgebra de $\mathcal{A}$ cujo universo é $Sg^{\mathcal{A}}(\emptyset)$.*

Diz-se que $\mathcal{A}$ ***é gerada por*** *X ou que X* ***é um conjunto de geradores de*** *$\mathcal{A}$ se $\mathcal{S}g^{\mathcal{A}}(X) = \mathcal{A}$. A álgebra $\mathcal{A}$ diz-se* ***finitamente gerada*** *se $\mathcal{A}$ admite um conjunto de geradores finito.*

Exemplo

O anel $\mathcal{Z} = (\mathbb{Z}; +, \cdot, -, 0)$ é finitamente gerado, pois $\mathcal{S}g^{\mathcal{Z}}(\{1\}) = \mathcal{Z}$.

Congruências e álgebras quociente

Uma congruência numa álgebra é uma relação de equivalência que é compatível com as operações da álgebra. A noção de congruência desempenha um papel relevante no estudo de Álgebra Universal.

Definição

Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma relação de equivalência em A. Diz-se que θ ***é uma congruência*** *em $\mathcal{A}$ se θ satisfaz a* ***propriedade de substituição****, i.e., se para quaisquer $n \in \tau(O)$, $f \in O_n$ e $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A^n$,*

$$(\forall i \in \{1, \dots, n\}, a_i \,\theta\, b_i) \Rightarrow f^{\mathcal{A}}(a_1, \dots, a_n) \,\theta\, f^{\mathcal{A}}(b_1, \dots, b_n).$$

Exemplo

(1) Considere o anel $(\mathbb{Z}; +, \cdot, -, 0)$. *Para cada* $q \in \mathbb{Z}$, *seja* $\equiv_q$ *a relação de equivalência definida em* $\mathbb{Z}$ *por*

$$r \equiv_q s \text{ sse } r - s = qk, \text{ para algum } k \in \mathbb{Z}.$$

Facilmente se verifica que:

(a) $\equiv_q$ *é uma congruência neste anel, para todo* $q \in \mathbb{Z}$.

(b) $\equiv_0$ *é a congruência identidade.*

(c) $\equiv_1$ *é a congruência universal.*

Exemplo

(2) Seja $\mathcal{A} = (\{a, b, c, d\}; f^{\mathcal{A}})$ *a álgebra de tipo* (1), *onde* $f^{\mathcal{A}}$ *é a operação unária definida por*

x	a	b	c	d
$f^{\mathcal{A}}(x)$	b	a	d	c

Para determinar todas as congruências de $\mathcal{A}$ *pode-se começar por determinar todas as partições de* $\{a, b, c, d\}$ *e seguidamente procurar as partições com a propriedade de que a imagem de uma classe é ainda uma classe. Relativamente à álgebra* $\mathcal{A}$, *conclui-se que as relações de congruência são as relações de equivalência associadas às seguintes partições*

$$\{\{a\}, \{b\}, \{c\}, \{d\}\}, \quad \{\{a\}, \{b\}, \{c, d\}\}, \quad \{\{a, b\}, \{c\}, \{d\}\},$$

$$\{\{a, b\}, \{c, d\}\}, \quad \{\{a, c\}, \{b, d\}\}, \quad \{\{a, d\}, \{b, c\}\}, \quad \{\{a, b, c, d\}\}.$$

Exemplo

(3) Dado um grupo $\mathcal{G} = (G; \cdot, ^{-1}, 1_G)$, podemos estabelecer uma relação entre as congruências de G e os subgrupos invariantes de G:

(a) se θ é uma congruência em $\mathcal{G}$, então $[1_G]_\theta$ é o universo de um subgrupo invariante de $\mathcal{G}$ e, dados $a, b \in G$, tem-se $a\,\theta\,b$ se e só se $a \cdot b^{-1} \in [1_G]_\theta$;

(b) se $\mathcal{N} = (N; \cdot, ^{-1}, 1_G)$ é um subgrupo invariante de $\mathcal{G}$, a relação binária θ definida em N por

$$a\,\theta\,b \text{ sse } a \cdot b^{-1} \in N$$

é uma congruência em $\mathcal{G}$ e tem-se $[1_G]_\theta = N$.

A aplicação $\theta \mapsto [1_G]_\theta$ é uma bijeção entre o conjunto das congruências de $\mathcal{G}$ e o conjunto dos subgrupos invariantes de $\mathcal{G}$.

Exemplo

(4) Se $\mathcal{R} = (R; \wedge, \vee)$ *é um reticulado, então* $\theta \in \mathrm{Eq}(R)$ *é uma congruência em* $\mathcal{R}$ *se e só se:*

(a) *cada classe de* θ *é um sub-reticulado;*

(b) *cada classe de* θ *é um subconjunto convexo de* R*;*

(c) *as classes de equivalência de* θ *são fechadas para quadriláteros (i.e. sempre que* a, b, c, d *são elementos de* R *distintos e tais que* $a < b$*,* $c < d$ *e*

$$(a \vee d = b \text{ e } a \wedge d = c) \text{ ou } (b \vee c = d \text{ e } b \wedge c = a),$$

então $a \,\theta\, b$ *sse* $c \,\theta\, d$*).*

O conjunto de todas as congruências da álgebra $\mathcal{A}$ é denotado por Cong($\mathcal{A}$).

A relação identidade $\triangle_A = \{(a,a) \in A^2 \mid a \in A\}$ e a relação universal $\nabla_A = A^2$ são elementos de Cong($\mathcal{A}$).

O conjunto de congruências de uma álgebra, quando ordenado pela relação de inclusão de conjuntos, define um reticulado. O estudo das propriedades deste reticulado fornece informação relevante no estudo da álgebra.

Lema

Sejam $\mathcal{A}$ uma álgebra. Se θ_1, θ_2 são congruências em $\mathcal{A}$, então:

(1) $\theta_1 \cap \theta_2 \in \mathrm{Cong}(\mathcal{A})$.

(2) $\theta_1 \vee \theta_2 = \{(x, y) \in A^2 \mid \exists\, n \in \mathbb{N}, \exists\, z_0, z_1, \dots, z_n \in A : x = z_0, y = z_n$ $e\ \forall 1 \leq k \leq n, z_{k-1}\, \theta_1\, z_k \text{ ou } z_{k-1}\, \theta_2\, z_k\} \in \mathrm{Cong}(\mathcal{A})$.

Teorema

Sejam $\mathcal{A}$ uma álgebra. Então $(\mathrm{Cong}(\mathcal{A}), \subseteq)$ *é um reticulado, tendo-se, para quaisquer* $\theta_1, \theta_2 \in \mathrm{Cong}(\mathcal{A})$,

$$\theta_1 \wedge \theta_2 = \theta_1 \cap \theta_2 \text{ e}$$

$$\theta_1 \vee \theta_2 = \{(x, y) \in A^2 \mid \exists\, n \in \mathbb{N}, \exists\, z_0, z_1, \dots, z_n \in A : x = z_0, y = z_n \\ e\ \forall 1 \leq k \leq n, z_{k-1}\, \theta_1\, z_k \text{ ou } z_{k-1}\, \theta_2\, z_k\}.$$

Definição

*Sejam $\mathcal{A}$ uma álgebra. Ao reticulado $\mathcal{Cong}(\mathcal{A}) = (\mathrm{Cong}(\mathcal{A}), \subseteq)$ dá-se a designação de **reticulado das congruências de** $\mathcal{A}$.*

Lema

Sejam $\mathcal{A}$ uma álgebra e $\{\theta_i\}_{i\in I}$ uma família de congruências em $\mathcal{A}$. Então $\bigcap_{i\in I} \theta_i$ é uma congruência em $\mathcal{A}$.

Teorema

Seja $\mathcal{A}$ uma álgebra. Então $\mathcal{Cong}(\mathcal{A})$ é um reticulado completo, tendo-se, para cada família $\{\theta_i\}_{i\in I}$ de congruências em $\mathcal{A}$,

$$\bigwedge_{i\in I} \theta_i = \bigcap_{i\in I} \theta_i \quad e \quad \bigvee_{i\in I} \theta_i = \bigcap \{\theta \in \mathrm{Cong}(\mathcal{A}) \mid \bigcup_{i\in I} \theta_i \subseteq \theta\}.$$

Dada uma álgebra $\mathcal{A} = (A; F)$ e $X \subseteq A \times A$, existe pelo menos uma congruência em $\mathcal{A}$ que contém X, mais precisamente, a congruência universal ∇_A.

Assim, a família de congruências $\{\theta \in \mathrm{Cong}(\mathcal{A}) \,|\, X \subseteq \theta\}$ é não vazia e recorrendo a esta família constroi-se a menor congruência em $\mathcal{A}$ que contém X.

Teorema

Sejam $\mathcal{A} = (A; F)$ uma álgebra e $X \subseteq A \times A$. Então $\bigcap\{\theta \in \mathrm{Cong}(\mathcal{A}) \,|\, X \subseteq \theta\} \in \mathrm{Cong}(\mathcal{A})$ e esta é a menor congruência em $\mathcal{A}$ que contém X.

Definição

Sejam $\mathcal{A} = (A; F)$ *uma álgebra,* $X \subseteq A \times A$ *e* $a, b \in A$*. Designa-se por* ***congruência gerada por*** X ***em*** $\mathcal{A}$*, e representa-se por* $\Theta(X)$*, a congruência* $\bigcap\{\theta \in \mathrm{Cong}(\mathcal{A}) \mid X \subseteq \theta\}$*.*
Se $X = \{(a_i, a_j) \in A \times A : 1 \leq i, j \leq n\}$*, representa-se* $\Theta(X)$ *por* $\Theta(a_1, \ldots, a_n)$*. Em particular, se* $X = \{(a, b)\}$*, designa-se por* ***congruência principal gerada por*** a, b ***em*** $\mathcal{A}$*, e representa-se por* $\Theta(a, b)$*, a congruência* $\bigcap\{\theta \in \mathrm{Cong}(\mathcal{A}) \mid a\,\theta\,b\}$*.*

Teorema

Seja $\mathcal{A}$ *uma álgebra. Então* $Cong(\mathcal{A})$ *é um reticulado algébrico. Os elementos compactos do reticulado* $Cong(\mathcal{A})$ *são as congruências finitamente geradas*

$$\Theta((a_1, b_1), \ldots, (a_n, b_n)).$$

Alguns factos úteis a respeito de congruências são estabelecidos no resultado seguinte.

Teorema

Sejam $\mathcal{A}$ *uma álgebra,* $a_1, b_1, \ldots, a_n, b_n \in A$ *e* $\theta \in \mathrm{Cong}(\mathcal{A})$*. Então*

(a) $\Theta(a_1, b_1) = \Theta(b_1, a_1)$.

(b) $\Theta((a_1, b_1), \ldots (a_n, b_n)) = \Theta(a_1, b_1) \vee \ldots \vee \Theta(a_n, b_n)$.

(c) $\Theta(a_1, \ldots, a_n) = \Theta(a_1, a_2) \vee \Theta(a_2, a_3) \vee \ldots \vee \Theta(a_{n-1}, a_n)$.

(d) $\theta = \bigcup\{\Theta(a, b) \mid (a, b) \in \theta\} = \bigvee\{\Theta(a, b) \mid (a, b) \in \theta\}$.

(e) $\theta = \bigcup\{\Theta((a_1, b_1), \ldots, (a_n, b_n)) \mid (a_i, b_i) \in \theta, n \geq 1\}$.

Os reticulados de congruências de certas classes de álgebras satisfazem propriedades adicionais que têm consequências nas propriedades das respetivas álgebras.

Definição

Sejam $\mathcal{A}$ *uma álgebra e* $\theta_1, \theta_2 \in \mathrm{Cong}(\mathcal{A})$. *Diz-se que* θ_1 *e* θ_2 *são* ***permutáveis*** *se* $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$. *Diz-se que a álgebra* $\mathcal{A}$ *é:*

- ***congruente-permutável*** *se qualquer par de congruências de* $\mathcal{A}$ *é permutável;*
- ***congruente-distributiva*** *(**congruente-modular**) se* $Cong(\mathcal{A})$ *é distributivo (modular).*

Uma classe $\mathbf{K}$ *de álgebras diz-se* ***congruente-permutavel***, ***congruente-distributiva***, ***congruente-modular*** *se cada álgebra da classe satisfaz a respetiva propriedade.*

Nos resultados seguintes apresentam-se algumas propriedades a respeito de congruências congruente-permutáveis.

Teorema

Sejam $\mathcal{A}$ uma álgebra e $\theta_1, \theta_2 \in \text{Cong}(\mathcal{A})$. Então as afirmações seguintes são equivalentes:

(a) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$,

(b) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$,

(c) $\theta_2 \circ \theta_1 \subseteq \theta_1 \circ \theta_2$.

Teorema

Seja $\mathcal{A}$ uma álgebra. Se $\mathcal{A}$ é congruente-permutável, então $\mathcal{A}$ é congruente-modular.

Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma congruência em $\mathcal{A}$.

Atendendo à propriedade de substituição satisfeita pela congruência θ, para cada $f \in O_n$, $n \in \tau(O)$, a correspondência de $(A/\theta)^n$ em A/θ que a cada elemento $([a_1]_\theta, \ldots, [a_n]_\theta)$ de $(A/\theta)^n$ associa o elemento $[f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta$ é independente dos representantes $a_1, \ldots, a_n$ que se escolhem para as classes $[a_1]_\theta$, ..., $[a_n]_\theta$, pelo que esta correspondência é uma operação n-ária em A/θ.

Assim, é possível associar ao conjunto quociente A/θ a estrutura de uma álgebra do mesmo tipo da álgebra $\mathcal{A}$.

Definição

*Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ) e θ uma congruência em $\mathcal{A}$. Chama-se **álgebra quociente de $\mathcal{A}$ por** θ, e representa-se por $\mathcal{A}/\theta$, a álgebra do mesmo tipo da álgebra $\mathcal{A}$, com universo A/θ e tal que, para cada $n \in \tau(O)$ e cada símbolo operacional $f \in O_n$,*

$$f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta) = [f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta, \ \forall (a_1, \ldots, a_n) \in A^n.$$

Exemplo

Consideremos o anel $\mathcal{Z} = (\mathbb{Z}; +^{\mathcal{Z}}, \cdot^{\mathcal{Z}})$, *onde* $+^{\mathcal{Z}}$ *e* $\cdot^{\mathcal{Z}}$ *são as operações usuais de adição e multiplicação em* $\mathbb{Z}$. *Para cada* $q \in \mathbb{N}$, *seja* $\equiv_q$ *a conguência em* $\mathcal{Z}$ *definida em* $\mathbb{Z}$ *por*

$$r \equiv_q s \text{ sse } r - s = qk, \text{ para algum } k \in \mathbb{Z}.$$

Para cada $q \in \mathbb{N}$, *a álgebra* $\mathcal{Z}/\equiv_q$ *é a álgebra* $(\mathbb{Z}/\equiv_q; +^{\mathcal{Z}/\equiv_q}, \cdot^{\mathcal{Z}/\equiv_q})$ *do tipo* $(2,2)$ *onde* $+^{\mathcal{Z}/\equiv_q}$ *e* $\cdot^{\mathcal{Z}/\equiv_q}$ *são as operaçoes binárias em* $\mathbb{Z}/\equiv_q$ *definidas por*

$$[a]_{\equiv_q} +^{\mathcal{Z}/\equiv_q} [b]_{\equiv_q} = [a +^{\mathcal{Z}} b]_{\equiv_q} \text{ e } [a]_{\equiv_q} \cdot^{\mathcal{Z}/\equiv_q} [b]_{\equiv_q} = [a \cdot^{\mathcal{Z}} b]_{\equiv_q},$$

para quaisquer $[a]_{\equiv_q}, [b]_{\equiv_q} \in \mathbb{Z}/\equiv_q$.

Homomorfismos

No estudo de aplicações entre álgebras do mesmo tipo são relevantes as que são compatíveis com as operações das álgebras: os homomorfismos.

Definição

Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo (O, τ) e $\alpha : A \to B$ uma função.

- *Dado um símbolo de operação $f \in O_n$, $n \in \mathbb{N}_0$, diz-se que α* ***é compatível com*** *f ou que α* ***respeita a interpretação de*** *f se*

$$\alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),$$

  para qualquer $(a_1, \ldots, a_n) \in A^n$.

- *Caso α seja compatível com todo o símbolo de operação de O, i.e., se, para cada $n \in \mathbb{N}_0$ e para cada $f \in O_n$, α* ***é compatível com*** *f, diz-se que α* ***é um homomorfismo*** *de $\mathcal{A}$ em $\mathcal{B}$ e escreve-se $\alpha : \mathcal{A} \to \mathcal{B}$.*

- *O conjunto dos homomorfismos de $\mathcal{A}$ em $\mathcal{B}$ é representado por* $\operatorname{Hom}(\mathcal{A}, \mathcal{B})$.

Exemplo

(1) Os homomorfismos de grupos, de anéis e de reticulados são casos particulares da definição anterior.

(2) A função $h : \mathbb{R} \to \mathbb{R}_0^+$*, que a cada real* x *associa o seu valor absoluto* $|x|$*, é um homomorfismo de* $(\mathbb{R}, \cdot)$ *em* $(\mathbb{R}_0^+, \cdot)$*, uma vez que, para quaisquer* $x, y \in \mathbb{R}$, $|x \cdot y| = |x| \cdot |y|$.

Exemplo

(3) Dado $n \in \mathbb{N}$*, representa-se por* $M_n(\mathbb{R})$ *o conjunto das matrizes reais quadradas de ordem* n *e por* $\mathcal{M}_n$ *a álgebra* $(M_n(\mathbb{R}); \cdot^{\mathcal{M}_n})$*, onde* $\cdot^{\mathcal{M}_n}$ *representa a multiplicação usual de matrizes de* $M_n(\mathbb{R})$*. É simples verificar que a aplicação* $h : M_n(\mathbb{R}) \to \mathbb{R}$*, que a cada matriz* $A \in M_n(\mathbb{R})$ *associa o seu determinante* $|A|$*, é um homomorfismo de* $\mathcal{M}_n$ *no semigrupo multiplicativo* $\mathcal{R} = (\mathbb{R}; \cdot^{\mathcal{R}})$ *(onde* $\cdot^{\mathcal{R}}$ *representa a multiplicação usual em* $\mathbb{R}$*).*

Exemplo

(4) Consideremos as álgebras

$$\mathcal{A}_3 = (\{(1),(123),(132)\}; \cdot^{\mathcal{A}_3}) \quad e \quad \mathcal{Z}_3 = (\{[1]_3,[2]_3,[3]_3\}; \cdot^{\mathcal{Z}_3}),$$

de tipo (2), *onde* $\cdot^{\mathcal{A}_3}$ *e* $\cdot^{\mathcal{Z}_3}$ *são, respetivamente, a operação de composição de permutações e a operação de adição usual em* $\mathbb{Z}_3$, *definidas pelas tabelas seguintes*

$\cdot^{\mathcal{A}_3}$	(1)	(123)	(132)
(1)	(1)	(123)	(132)
(123)	(123)	(132)	(1)
(132)	(132)	(1)	(123)

$\cdot^{\mathcal{Z}_3}$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Exemplo (continuação)

A partir das tabelas anteriores é simples perceber que a função

$$h : \{(1), (123), (132)\} \to \{[1]_3, [2]_3, [0]_3\},$$

definida por $(1) \mapsto [0]_3$, $(123) \mapsto [1]_3$, $(132) \mapsto [2]_3$, respeita a interpretação do símbolo de operação das álgebras e, portanto, h é um homomorfismo de $\mathcal{A}_3$ em $\mathcal{Z}_3$.

Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\alpha \in \mathrm{Hom}(\mathcal{A}, \mathcal{B})$.

- Se α é uma aplicação sobrejetiva diz-se que α é um ***epimorfismo***.

- O homomorfismo α diz-se um ***monomorfismo*** ou um ***mergulho*** de $\mathcal{A}$ em $\mathcal{B}$ se α é injetivo. Caso exista um mergulho de $\mathcal{A}$ em $\mathcal{B}$ diz-se que ***a álgebra*** $\mathcal{A}$ ***pode ser mergulhada na álgebra*** $\mathcal{B}$.

- A um homomorfismo que seja bijetivo dá-se a designação de ***isomorfismo***. Diz-se que a álgebra $\mathcal{A}$ ***é isomorfa à álgebra*** $\mathcal{B}$ se existe um isomorfismo de $\mathcal{A}$ em $\mathcal{B}$. Caso exista um isomorfismo de $\mathcal{A}$ em $\mathcal{B}$, também existe um isomorfismo de $\mathcal{B}$ em $\mathcal{A}$, pelo que, caso exista um isomorfismo de uma álgebra na outra, diz-se apenas que as álgebras $\mathcal{A}$ e $\mathcal{B}$ são isomorfas e escreve-se $\mathcal{A} \cong \mathcal{B}$.

- A um homomorfismo de $\mathcal{A}$ em $\mathcal{A}$ dá-se a designação de ***endomorfismo***. Um endomorfismo que seja bijetivo diz-se um ***automorfismo***.

Exemplo

O homomorfismo de $\mathcal{A}_3$ em $\mathcal{Z}_3$ definido no exemplo anterior é um isomorfismo, pelo que as álgebras $\mathcal{A}_3$ e $\mathcal{Z}_3$ são isomorfas.

Elementos de álgebra universal

Um isomorfismo é uma correspondência bijetiva entre os elementos de duas álgebras do mesmo tipo que respeita a interpretação de cada símbolo operacional.

Assim, há certas propriedades, ditas "propriedades algébricas", que sendo satisfeitas por uma dada álgebra são satisfeitas por qualquer álgebra que lhe seja isomorfa, o que torna as álgebras indistinguíveis a respeito destas propriedades.

Embora duas álgebras isomorfas possam ser completamente diferentes, em particular no que respeita aos seus elementos, é usual dizer que "as álgebras são a mesma, a menos de isomorfismo".

A composição de dois homomorfismos, desde que esteja definida, é ainda um homomorfismo.

Teorema

Sejam $\mathcal{A}, \mathcal{B}$ *e* $\mathcal{C}$ *álgebras do mesmo tipo. Se* $\alpha : \mathcal{A} \to \mathcal{B}$ *e* $\beta : \mathcal{B} \to \mathcal{C}$ *são homomorfismos (respetivamente, isomorfismos), então* $\beta \circ \alpha$ *é um homomorfismo (respetivamente, isomorfismo) de* $\mathcal{A}$ *em* $\mathcal{C}$*.*

O conjunto de endomorfismos de $\mathcal{A}$ representa-se por End$\mathcal{A}$ e o conjunto dos automorfismos de $\mathcal{A}$ representa-se por Aut$\mathcal{A}$.

Do resultado anterior segue que, para cada álgebra $\mathcal{A}$, cada um dos conjuntos End$\mathcal{A}$ e Aut$\mathcal{A}$ é fechado para a composição de aplicações. Assim, considerando que, para cada álgebra $\mathcal{A}$, a aplicação identidade id_A pertence quer a End$\mathcal{A}$ quer a Aut$\mathcal{A}$ e a aplicação inversa de um automorfismo de $\mathcal{A}$ é também um automorfismo de $\mathcal{A}$, segue que;

- $\mathcal{E}nd\mathcal{A} = (\mathrm{End}\mathcal{A}; \circ, \mathrm{id}_A)$ é um monóide;
- $\mathcal{A}ut\mathcal{A} = (\mathrm{Aut}\mathcal{A}; \circ, ^{-1}, \mathrm{id}_A)$, onde $^{-1}$ representa a operação unária que a cada automorfismo de Aut$\mathcal{A}$ associa a sua aplicação inversa, é um grupo.

Teorema

Sejam $\mathcal{A} = (A; F)$ *e* $\mathcal{B} = (B; G)$ *álgebras do mesmo tipo. Se a álgebra* $\mathcal{A}$ *é gerada por um conjunto* X *(*$X \subseteq A$*) e* $\alpha, \beta : \mathcal{A} \to \mathcal{B}$ *são homomorfismos tais que, para todo* $x \in X$, $\alpha(x) = \beta(x)$, *então* $\alpha = \beta$.

Demonstração.

Se a álgebra $\mathcal{A}$ é gerada pelo conjunto X, então $A = \bigcup_{i \in \mathbb{N}_0} X_i$, onde X_i são os conjuntos definidos indutivamente por

$$\begin{array}{rcl} X_0 & = & X; \\ X_{i+1} & = & X_i \cup \{f(x) \,|\, f \text{ é operação } n\text{-ária em } \mathcal{A} \text{ e } x \in (X_i)^n, n \in \mathbb{N}_0\}. \end{array}$$

Por indução em i prova-se que, para todo $i \in \mathbb{N}_0$, $\alpha(x) = \beta(x)$, para qualquer $x \in X_i$. Por conseguinte, para todo $x \in A$, $\alpha(x) = \beta(x)$ e, portanto, $\alpha = \beta$. $\square$

Teorema

Sejam $\mathcal{A} = (A; F)$, $\mathcal{B} = (B; G)$ *álgebras do mesmo tipo e* $\alpha : \mathcal{A} \to \mathcal{B}$ *um homomorfismo.*

(i) *Se* A_1 *é um subuniverso de* $\mathcal{A}$, *então* $\alpha(A_1)$ *é um subuniverso de* $\mathcal{B}$.

(ii) *Se* B_1 *é um subuniverso de* $\mathcal{B}$, *então* $\alpha^{\leftarrow}(B_1)$ *é um subuniverso de* $\mathcal{A}$.

Corolário

Sejam $\mathcal{A} = (A; F)$, $\mathcal{B} = (B; G)$ *álgebras de tipo* (O, τ) *e* $\alpha : \mathcal{A} \to \mathcal{B}$ *um homomorfismo. Então:*

(i) *Se* $\mathcal{A}_1 = (A_1; F_1)$ *é uma subálgebra de* $\mathcal{A}$, *então o par*

$$(\alpha(A_1); (f^{\alpha(\mathcal{A}_1)})_{f \in O}),$$

onde, para quaisquer $n \in \tau(O)$ *e* $f \in O_n$, $f^{\alpha(\mathcal{A}_1)}$ *é a função de* $\alpha(A_1)^n$ *em* $\alpha(A_1)$ *definida por*

$$f^{\alpha(\mathcal{A}_1)}(\alpha(a_1), \ldots, \alpha(a_n)) = f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),$$

para qualquer $(a_1, \ldots, a_n) \in (A_1)^n$, *é uma subálgebra de* $\mathcal{B}$.

(ii) Se $\mathcal{B}_1 = (B_1, G_1)$ é uma subálgebra de $\mathcal{B}$ e $\alpha^{\leftarrow}(B_1) \neq \emptyset$, então o par

$$(\alpha^{\leftarrow}(B_1); (f^{\alpha^{\leftarrow}(\mathcal{B}_1)})_{f \in O}),$$

onde, para quaisquer $n \in \tau(O)$ e $f \in O_n$, $f^{\alpha^{\leftarrow}(\mathcal{B}_1)}$ é a correspondência de $(\alpha^{\leftarrow}(B_1))^n$ em $\alpha^{\leftarrow}(B_1)$ definida por

$$f^{\alpha^{\leftarrow}(\mathcal{B}_1)}(a_1, \ldots, a_n) = f^{\mathcal{A}}(a_1, \ldots, a_n),$$

para qualquer $(a_1, \ldots, a_n) \in (\alpha^{\leftarrow}(B_1))^n$, é uma subálgebra de $\mathcal{A}$.

(iii) Para qualquer $X \subseteq A$, $\mathcal{S}g^{\mathcal{B}}(\alpha(X)) = \alpha(\mathcal{S}g^{\mathcal{A}}(X))$.

Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ são álgebras do mesmo tipo (O, τ), $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo, $\mathcal{A}_1 = (A_1; F_1)$ uma subálgebra de $\mathcal{A}$ e $\mathcal{B}_1 = (B_1; G_1)$ uma subálgebra de $\mathcal{B}$ tal que $\alpha^{\leftarrow}(B_1) \neq \emptyset$. Dá-se a designação de:

- ***imagem homomorfa de*** $\mathcal{A}_1$ à álgebra

$$\alpha(\mathcal{A}_1) = (\alpha(A_1); (f^{\alpha(\mathcal{A}_1)})_{f \in O});$$

- ***pré-imagem de*** $\mathcal{B}_1$ à álgebra

$$\alpha^{\leftarrow}(\mathcal{B}_1) = (\alpha^{\leftarrow}(B_1); (f^{\alpha^{\leftarrow}(\mathcal{B}_1)})_{f \in O}).$$

Observe-se que a álgebra $\mathcal{B}$ é uma imagem homomorfa de $\mathcal{A}$ se e só se existe um epimorfismo de $\mathcal{A}$ em $\mathcal{B}$.

Dado um homomorfismo α entre álgebras $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$, a aplicação $\alpha : A \to B$ não é, em geral, injetiva. Sendo assim, tem interesse estudar a relação binária induzida por α, ou seja, a que relaciona elementos que tenham a mesma imagem através da aplicação α.

Definição

*Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Designa-se por **kernel de** α, e representa-se por* $\ker \alpha$, *a relação binária em A definida por*

$$\ker \alpha = \{(a, b) \in A^2 : \alpha(a) = \alpha(b)\}.$$

Teorema

Sejam $\mathcal{A} = (A; F)$ *e* $\mathcal{B} = (B; G)$ *álgebras do mesmo tipo e* $\alpha : \mathcal{A} \to \mathcal{B}$ *um homomorfismo. Então a relação* $\ker \alpha$ *é uma congruência em* $\mathcal{A}$.

Demonstração.

É imediato que ker α é uma relação de equivalência em A. Além disso, para quaisquer $n \in \tau(O)$ e $f \in O_n$, se $(a_i, b_i) \in \ker \alpha$, $1 \leq i \leq n$, então

$$\begin{array}{rcl}\alpha(f^{\mathcal{A}}(a_1, \dots, a_n)) & = & f^{\mathcal{B}}(\alpha(a_1), \dots, \alpha(a_n)) \\ & = & f^{\mathcal{B}}(\alpha(b_1), \dots, \alpha(b_n)) \\ & = & \alpha(f^{\mathcal{A}}(b_1, \dots, b_n))\end{array}$$

e, portanto, $(f^{\mathcal{A}}(a_1, \dots, a_n), f^{\mathcal{A}}(b_1, \dots, b_n)) \in \ker \alpha$. Logo ker α é uma congruência em $\mathcal{A}$. $\square$

Do teorema anterior ressulta que a cada homomorfismo é possivel associar uma congruência. Reciprocamente, a cada congruência também é possível associar um homomorfismo.

Teorema

Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. A correspondência π_θ de A em A/θ, definida por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$, é uma aplicação.

Definição

*Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. A aplicação $\pi_\theta : A \to A/\theta$, definida por $\pi_\theta(a) = [a]_\theta$, é designada por **aplicação natural de** A **em** A/θ.*

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* θ *uma congruência em* $\mathcal{A}$. *Então a aplicação* $\pi_\theta : A \to A/\theta$, *definida por* $\pi_\theta(a) = [a]_\theta$, *para todo* $a \in A$, *é um epimorfismo de* $\mathcal{A}$ *em* $\mathcal{A}/\theta$. *Além disso, tem-se* $\ker \pi_\theta = \theta$.

Demonstração.

Sejam $\theta \in \mathrm{Cong}(\mathcal{A})$ e $\pi_\theta : A \to A/\theta$ a aplicação definida por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$. Então, para quaisquer $n \in \tau(O)$, $f \in O_n$ e $(a_1, \dots, a_n) \in A^n$, tem-se

$$\begin{array}{rcl} \pi_\theta(f^{\mathcal{A}}(a_1, \dots, a_n)) & = & [f^{\mathcal{A}}(a_1, \dots, a_n)]_\theta \\ & = & f^{\mathcal{A}/\theta}([a_1]_\theta, \dots, [a_n]_\theta) \\ & = & f^{\mathcal{A}/\theta}(\pi_\theta(a_1), \dots, \pi_\theta(a_n)), \end{array}$$

pelo que π_θ é um homomorfismo. Claramente, π_θ é sobrejetiva. A prova da igualdade $\ker \pi_\theta = \theta$ é imediata, pois, para qualquer $(a, b) \in A \times A$,

$$(a, b) \in \ker \pi_\theta \Leftrightarrow \pi_\theta(a) = \pi_\theta(b) \Leftrightarrow [a]_\theta = [b]_\theta \Leftrightarrow (a, b) \in \theta.$$

$\square$

Definição

*Sejam $\mathcal{A} = (A; F)$ uma álgebra e θ uma congruência em $\mathcal{A}$. O epimorfismo $\pi_\theta : \mathcal{A} \to \mathcal{A}/\theta$, definido por $\pi_\theta(a) = [a]_\theta$, para todo $a \in A$, é designado por **homomorfismo natural de $\mathcal{A}$ em $\mathcal{A}/\theta$**.*

Sendo $\mathcal{A} = (A; F)$ uma álgebra, θ uma congruência em $\mathcal{A}$ e π_θ o epimorfismo definido anteriormente, tem-se $\ker \pi_\theta = \theta$. Assim, dos dois teoremas anteriores resulta que as congruências numa álgebra $\mathcal{A}$ são exatamente os kernels dos homomorfismos com domínio $\mathcal{A}$.

Sejam $\mathcal{A}$ e $\mathcal{B}$ álgebras do mesmo tipo e $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Vimos anteriormente que $\ker \alpha$ é uma congruência em $\mathcal{A}$, pelo que faz sentido considerar a álgebra quociente $\mathcal{A}/\ker \alpha$ e o epimorfismo natural $\pi_{\ker \alpha} : \mathcal{A} \to \mathcal{A}/\ker \alpha$. Assim, temos duas imagens homomórficas de $\mathcal{A}$: $\alpha(\mathcal{A})$ e $\pi_{\ker \alpha}(\mathcal{A})$. O teorema seguinte estabelece a relação existente entre estas imagens homomórficas de $\mathcal{A}$.

Elementos de álgebra universal

Sendo $\mathcal{A}$ e $\mathcal{B}$ álgebras do mesmo tipo, $\alpha : \mathcal{A} \to \mathcal{B}$ um epimorfismo e $\theta = \ker \alpha$, pode estabelecer-se um isomorfismo entre $\mathcal{A}/\theta$ e $\mathcal{B}$.

Teorema (Teorema do Homomorfismo)

Sejam $\mathcal{A} = (A; F)$ e $\mathcal{B} = (B; G)$ álgebras do mesmo tipo, $\alpha : \mathcal{A} \to \mathcal{B}$ um homomorfismo, $\theta = \ker \alpha$ e $\pi_\theta : \mathcal{A} \to \mathcal{A}/\theta$ o homomorfismo natural. Então a correspondência β de A/θ para B, definida por $\beta([a]_\theta) = \alpha(a)$, para todo $[a]_\theta \in A/\theta$, é um monomorfismo de $\mathcal{A}/\theta$ em $\mathcal{B}$ e tem-se $\beta \circ \pi_\theta = \alpha$. Caso α seja um epimorfismo, então β é um isomorfismo.

$$\begin{tikzcd}
\mathcal{A} \arrow[r, "\alpha"] \arrow[d, "\pi_\theta"'] & \mathcal{B} \\
\mathcal{A}/\theta \arrow[ur, "\beta"'] &
\end{tikzcd}$$

Demonstração

A correspondência β é uma aplicação. Com efeito, para todo $[a]_\theta \in A/\theta$, tem-se $\beta([a]_\theta) \in B$ e, para quaisquer $[a]_\theta, [b]_\theta \in A/\theta$,

$$[a]_\theta = [b]_\theta \Rightarrow a\,\theta\,b \Rightarrow \alpha(a) = \alpha(b) \Rightarrow \beta([a]_\theta) = \beta([b]_\theta).$$

Facilmente também se prova que β é injetiva, pois, para quaisquer $[a]_\theta, [b]_\theta \in A/\theta$,

$$\beta([a]_\theta) = \beta([b]_\theta) \Rightarrow \alpha(a) = \alpha(b) \Rightarrow a\,\theta\,b \Rightarrow [a]_\theta = [b]_\theta.$$

A aplicação β é um homomorfismo, uma vez que, para qualquer símbolo de operação n-ário f e para qualquer $(a_1, \ldots, a_n) \in A^n$,

$$\begin{array}{rcl}\beta(f^{\mathcal{A}/\theta}([a_1]_\theta, \ldots, [a_n]_\theta)) & = & \beta([f^{\mathcal{A}}(a_1, \ldots, a_n)]_\theta) \\ & = & \alpha(f^{\mathcal{A}}(a_1, \ldots, a_n)) \\ & = & f^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)) \\ & = & f^{\mathcal{B}}(\beta([a_1]_\theta), \ldots, \beta([a_n]_\theta)).\end{array}$$

Demonstração.

Assim, β é um monomorfismo.

A prova da igualdade $\beta \circ \pi_\theta = \alpha$ é imediata, pois $\beta \circ \pi_\theta$ e α são ambas aplicações de A em B e, para qualquer $a \in A$,

$$(\beta \circ \pi_\theta)(a) = \beta(\pi_\theta(a)) = \beta([a]_\theta) = \alpha(a).$$

Caso α seja um epimorfismo é simples concluir que β é um isomorfismo. De facto, se α é sobrejetiva, então, para todo $b \in B$, existe $a \in A$ tal que $b = \alpha(a)$ e, por conseguinte, $b = \beta([a]_\theta)$; logo β também é sobrejetiva. $\square$

O Teorema do Homomorfismo é também conhecido por Primeiro Teorema do Isomorfismo.

Do Teorema do Homomorfismo segue que uma álgebra é imagem homomorfa de outra álgebra se e só se é isomorfa a uma álgebra quociente de $\mathcal{A}$. Assim, o problema da determinação das imagens homomorfas de $\mathcal{A}$ reduz-se ao problema da determinação das congruencias de $\mathcal{A}$.

Definição

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $\theta, \phi \in \mathrm{Cong}(\mathcal{A})$ *tais que* $\theta \subseteq \phi$. *Define-se a relação* ϕ/θ *em* A/θ *por*

$$\phi/\theta = \{([a]_\theta, [b]_\theta) \in (A/\theta)^2 \mid (a, b) \in \phi\}.$$

Lema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $\theta, \phi \in \mathrm{Cong}(\mathcal{A})$ *tais que* $\theta \subseteq \phi$. *Então* ϕ/θ *é uma congruência em* $\mathcal{A}/\theta$.

Teorema (Teorema da Correspondência)

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $\theta \in \mathrm{Cong}(\mathcal{A})$. *Então o sub-reticulado* $\mathbf{[}\theta, \nabla_A\mathbf{]}$ *de* $\mathrm{Cong}(\mathcal{A})$ *e o reticulado* $Cong(\mathcal{A}/\theta)$ *são isomorfos. Mais precisamente, a correspondência* α *de* $[\theta, \nabla_A]$ *para* $\mathrm{Cong}(A/\theta)$, *definida por* $\alpha(\phi) = \phi/\theta$, *é um isomorfismo de reticulados de* $\mathbf{[}\theta, \nabla_A\mathbf{]}$ *em* $\mathrm{Cong}(\mathcal{A}/\theta)$.

Produtos diretos e álgebras diretamente indecomponíveis

Nas secções anteriores estudámos três formas de construir novas álgebras a partir de álgebras dadas, nomeadamente a formação de subálgebras, de álgebras quociente e de imagens homomorfas.

Nesta secção abordamos um outro processo de construção de álgebras: a formação de produtos diretos de álgebras.

Note-se que com a formação de subálgebras, de álgebras quociente ou de imagens homomorfas a partir de uma dada álgebra, não é possível obter álgebras com uma cardinalidade superior à cardinalidade da álgebra inicial, mas com a formação de produtos diretos tal já é possível.

Sejam I um conjunto e $(A_i)_{i\in I}$ uma família de conjuntos.

Designa-se por ***produto cartesiano*** da família $(A_i)_{i\in I}$, e representa-se por $\prod_{i\in I} A_i$, o conjunto de todas as funções f de I em $\bigcup_{i\in I} A_i$ tais que, para todo $i \in I$, $f(i) \in A_i$, i.e.,

$$\prod_{i\in I} A_i = \left\{f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i, \forall i \in I\right\}.$$

Cada conjunto A_i designa-se por ***fator*** do produto cartesiano.

Se $A_i = \emptyset$, para algum $i \in I$, tem-se $\prod_{i\in I} A_i = \emptyset$.

No caso em que $I = \emptyset$, o conjunto $\prod_{i\in I} A_i$ tem exatamente um elemento, a função vazia; i.e., $\prod_{i\in I} A_i = \{\emptyset\}$.

Se $A_i = A$, para todo $i \in I$, representa-se $\prod_{i \in I} A_i$ por A^I.

No sentido de relacionar a definição de produto cartesiano da família $(A_i)_{i \in \{1,2,\ldots,n\}}$ com a definição de $A_1 \times A_2 \ldots \times A_n$, convenciona-se o uso do n-uplo $(a_1, a_2, \ldots, a_n)$ de elementos de A como uma representação da função $f \in A^{\{1,2,\ldots,n\}}$ tal que $a_1 = f(1)$, $a_2 = f(2)$, $\ldots$, $a_n = f(n)$. Assim, $A_1 \times A_2 \times \ldots \times A_n = \prod_{i \in \{1,2,\ldots,n\}} A_i$.

Para cada $j \in I$, designa-se por ***projeção-j*** a aplicação $p_j : \prod_{i \in I} A_i \to A_j$ tal que $p_j(f) = f(j)$, para todo $f \in \prod_{i \in I} A_i$.

Definição

*Sejam I um conjunto e $(\mathcal{A}_i)_{i\in I} = ((A_i; F_i))_{i\in I}$ uma família de álgebras do mesmo tipo (O, τ). Designa-se por **produto direto** da famíla $(\mathcal{A}_i)_{i\in I}$, e representa-se por $\prod_{i\in I}\mathcal{A}_i$, a álgebra de tipo (O, τ) com universo $\prod_{i\in I} A_i$ e tal que, para todo o símbolo de operação $f \in O_n$ e para quaisquer $f_1, \ldots, f_n \in \prod_{i\in I} A_i$, se tem*

$$f^{\prod_{i\in I}\mathcal{A}_i}(f_1, \ldots, f_n)(i) = f^{\mathcal{A}_i}(f_1(i), \ldots, f_n(i)), \text{ para todo } i \in I.$$

Se $I = \{i_1, \ldots, i_k\}$, o produto direto $\prod_{i \in I} \mathcal{A}_i$ é representado por $\mathcal{A}_{i_1} \times \ldots \times \mathcal{A}_{i_k}$.

No caso em que $\mathcal{A}_i = \mathcal{A}$, para todo $i \in I$, $\prod_{i \in I} \mathcal{A}_i$ é representado por $\mathcal{A}^I$ e diz-se uma potência direta de $\mathcal{A}$.

Se $I = \emptyset$, $\prod_{i \in I} \mathcal{A}_i$ é a álgebra trivial com universo $\{\emptyset\}$.

Teorema

Se $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$ são álgebras do mesmo tipo, então:

(i) $\mathcal{A}_1 \times \mathcal{A}_2 \cong \mathcal{A}_2 \times \mathcal{A}_1$.

(ii) $\mathcal{A}_1 \times (\mathcal{A}_2 \times \mathcal{A}_3) \cong (\mathcal{A}_1 \times \mathcal{A}_2) \times \mathcal{A}_3$.

Para todo $j \in I$, a projeção $p_j : \prod_{i \in I} A_i \to A_j$ é um epimorfismo de $\prod_{i \in I} \mathcal{A}_i$ em $\mathcal{A}_j$. Assim, cada uma das álgebras $\mathcal{A}_j$, $j \in I$, é imagem homomorfa de $\prod_{i \in I} \mathcal{A}_i$.

Teorema

Sejam $(\mathcal{A}_i)_{i\in I} = ((A_i; F_i))_{i\in I}$ *uma família de álgebras do mesmo tipo e* $\mathcal{A} = (A; F)$ *uma subálgebra de* $\prod_{i\in I} \mathcal{A}_i$*. Então* $\bigcap_{i\in I}(\ker p_i)_{|A} = \triangle_A$*.*

Demonstração.

Seja $(a, b) \in \bigcap_{i\in I}(\ker p_i)_{|A}$. Então $a, b \in A \subseteq \prod_{i\in I} A_i$ e, para todo $i \in I$, $p_i(a) = p_i(b)$. Logo $a = b$ e, portanto, $(a, b) \in \triangle_A$.
Reciprocamente, é óbvio que $\triangle_A \subseteq (\ker p_i)_{|A}$, para todo $i \in I$. $\square$

Lema

Sejam $\mathcal{A}_1 = (A_1; F_1)$ *e* $\mathcal{A}_2 = (A_2; F_2)$ *álgebras do mesmo tipo,* $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ *e* $p_i : A_1 \times A_2 \to A_i$ *a projeção-*i*,* $i \in \{1, 2\}$*. Em* $\mathrm{Cong}(\mathcal{A})$*, tem-se:*

(i) $\ker\, p_1 \cap \ker p_2 = \triangle_{A_1 \times A_2}$.

(ii) $\ker\, p_1 \circ \ker p_2 = \ker\, p_2 \circ \ker p_1$.

(iii) $\ker\, p_1 \vee \ker p_2 = \nabla_{A_1 \times A_2}$.

Demonstração.

(i) Imediato a partir da proposição anterior.

(ii) Para quaisquer $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$, tem-se

$$((a_1, a_2), (b_1, a_2)) \in \ker p_2 \text{ e } ((b_1, a_2), (b_1, b_2)) \in \ker p_1.$$

pelo que $((a_1, a_2), (b_1, b_2)) \in \ker p_1 \circ \ker p_2$. Logo $\ker p_1 \circ \ker p_2 = \nabla_{A_1 \times A_2}$. De modo análogo prova-se que $\ker p_2 \circ \ker p_1 = \nabla_{A_1 \times A_2}$. Assim, $\ker\, p_1 \circ \ker p_2 = \ker\, p_2 \circ \ker p_1$.

(iii) Uma vez que $\ker p_1$ e $\ker p_2$ são permutáveis, então $\ker p_1 \vee \ker p_2 = \ker p_1 \circ \ker p_2$ e da prova de (ii) segue que $\ker p_1 \vee \ker p_2 = \nabla_{A_1 \times A_2}$. □

O resultado anterior motiva a definição seguinte.

Definição

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* $\theta_1 \in \mathrm{Cong}(\mathcal{A})$. *Diz-se que* θ_1 *é uma* ***congruência fator*** *se existe uma congruência* θ_2 *em* $\mathcal{A}$ *tal que* $\theta_1 \cap \theta_2 = \triangle_A$, $\theta_1 \vee \theta_2 = \nabla_A$ *e* θ_1 *e* θ_2 *são permutáveis. O par* (θ_1, θ_2) *diz-se um* ***par de congruências fator em*** $\mathcal{A}$.

Do lema anterior sabe-se que a álgebra resultante do produto direto de duas álgebras tem sempre duas congruências fator. Reciprocamente, o próximo resultado estabelece que se uma álgebra tem um par de congruências fator, então esta álgebra é isomorfa a um produto direto de duas álgebras.

Teorema

Sejam $\mathcal{A} = (A; F)$ *uma álgebra e* (θ_1, θ_2) *um par de congruências fator em* $\mathcal{A}$*. Então a aplicação* $\varphi : A \to A/\theta_1 \times A/\theta_2$*, definida por* $\varphi(a) = ([a]_{\theta_1}, [a]_{\theta_2})$*, para todo* $a \in A$*, é um isomorfismo de* $\mathcal{A}$ *em* $\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2$*.*

Demonstração

Claramente, φ é uma aplicação.

De forma simples verifica-se que a aplicação φ é injetiva: dados $a, b \in A$ tais que $\varphi(a) = \varphi(b)$, tem-se $[a]_{\theta_1} = [b]_{\theta_1}$ e $[a]_{\theta_2} = [b]_{\theta_2}$. Logo $(a, b) \in \theta_1$ e $(a, b) \in \theta_2$, donde $a = b$.

A aplicação φ também é sobrejetiva. De facto, dados $a, b \in A$, existe $c \in A$ tal que $(a, c) \in \theta_1$ e $(c, b) \in \theta_2$. Então $([a]_{\theta_1}, [b]_{\theta_2}) = ([c]_{\theta_1}, [c]_{\theta_2}) = \varphi(c)$.

Demonstração.

Por último, prova-se que φ é um homomorfismo, uma vez que, para todo o símbolo operacional f que seja n-ário e para quaisquer $a_1, \ldots, a_n \in A$, tem-se

$$\begin{array}{rcl}
\varphi(f^{\mathcal{A}}(a_1, \ldots, a_n)) & = & ([f^{\mathcal{A}}(a_1, \ldots, a_n)]_{\theta_1}, [f^{\mathcal{A}}(a_1, \ldots, a_n)]_{\theta_2}) \\
& = & (f^{\mathcal{A}/\theta_1}([a_1]_{\theta_1}, \ldots, [a_n]_{\theta_1}), f^{\mathcal{A}/\theta_2}([a_1]_{\theta_2}, \ldots, [a_n]_{\theta_2})) \\
& = & f^{\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2}(([a_1]_{\theta_1}, [a_1]_{\theta_2}), \ldots, ([a_n]_{\theta_1}, [a_n]_{\theta_2})) \\
& = & f^{\mathcal{A}/\theta_1 \times \mathcal{A}/\theta_2}(\varphi(a_1), \ldots, \varphi(a_n)).
\end{array}$$

$\square$

O resultado anterior mostra que é possível recorrer a certas congruências de uma álgebra para expressá-la como um produto direto de álgebras possívelmente mais pequenas. Porém, em certos casos só é possível expressar uma álgebra como um produto direto de álgebras se um dos fatores do produto direto for a própria álgebra.

Definição

*Seja $\mathcal{A}$ uma álgebra. Diz-se que $\mathcal{A}$ é **diretamente indecomponível** se sempre que $\mathcal{A} \cong \mathcal{A}_1 \times \mathcal{A}_2$, então $\mathcal{A}_1$ é a álgebra trivial ou $\mathcal{A}_2$ é uma álgebra trivial.*

Exemplo

Toda a álgebra finita com um número primo de elementos é diretamente indecomponível.

Corolário

Seja $\mathcal{A}$ uma álgebra. Então $\mathcal{A}$ é diretamente indecomponível se e só se as únicas congruências fator de $\mathcal{A}$ são $\triangle_A$ e ∇_A.

O resultado seguinte estabelece que as álgebras diretamente indecomponíveis funcionam como "blocos de construção" de certas álgebras.

Teorema

Toda a álgebra finita é isomorfa a um produto direto de álgebras diretamente indecomponíveis.

Demonstração

Seja $\mathcal{A} = (A; F)$ uma álgebra finita. A prova segue por indução forte no número de elementos de A.

Se $|A| = 1$, ou seja, se $\mathcal{A}$ é trivial, o resultado é imediato, uma vez que $\mathcal{A}$ é diretamente indecomponível.

Se $\mathcal{A}$ não é trivial, admita-se, por hipótese de indução, que toda álgebra $\mathcal{B} = (B; G)$ tal que $|B| < |A|$ é isomorfa a um produto direto de álgebras diretamente indecomponíveis.

Se $\mathcal{A}$ é diretamente indecomponível, a prova termina.

Demonstração.

Se $\mathcal{A}$ não é diretamente indecomponível, então existem álgebras não triviais $\mathcal{A}_1$ e $\mathcal{A}_2$ tais que $\mathcal{A} \cong \mathcal{A}_1 \times \mathcal{A}_2$. Uma vez que $|A_1|, |A_2| < |A|$ segue, por hipótese de indução, que

$$\begin{array}{rcl} \mathcal{A}_1 & \cong & \mathcal{B}_1 \times \ldots \times \mathcal{B}_m \\ \mathcal{A}_2 & \cong & \mathcal{C}_1 \times \ldots \times \mathcal{C}_n, \end{array}$$

onde $\mathcal{B}_1, \ldots, \mathcal{B}_m, \mathcal{C}_1, \ldots, \mathcal{C}_n$ são álgebras diretamente indecomponíveis. Consequentemente,

$$\mathcal{A} \cong \mathcal{B}_1 \times \ldots \times \mathcal{B}_m \times \mathcal{C}_1 \times \ldots \times \mathcal{C}_n.$$

$\square$

Utilizando produtos diretos, existem dois processos de obter um homomorfismo a partir de uma família de homomorfismos.

Teorema

Sejam $\mathcal{A}$ uma álgebra, $(\mathcal{A}_i)_{i\in I}$ e $(\mathcal{B}_i)_{i\in I}$ famílias de álgebras do mesmo tipo de $\mathcal{A}$ e $(h_i : \mathcal{A} \to \mathcal{B}_i)_{i\in I}$ e $(g_i : \mathcal{A}_i \to \mathcal{B}_i)_{i\in I}$ famílias de homomorfismos. Então

(i) *A aplicação $h : A \to \prod_{i\in I} B_i$, definida por $(h(a))(i) = h_i(a)$, para todo $a \in A$ e para todo $i \in I$, é um homomorfismo de $\mathcal{A}$ em $\prod_{i\in I} \mathcal{B}_i$.*

(ii) *A aplicação $g : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$, definida por $(g(a))(i) = g_i(a(i))$, para todo $a \in \prod_{i\in I} A_i$ e para todo $i \in I$, é um homomorfismo de $\prod_{i\in I} \mathcal{A}_i$ em $\prod_{i\in I} \mathcal{B}_i$.*

Produtos subdiretos e álgebras subdiretamente irredutíveis

Embora toda a álgebra finita seja isomorfa a um produto direto de álgebras diretamente indecomponíveis, o mesmo não acontece para álgebras infinitas em geral; por exemplo, as álgebras de Boole numeráveis infinitas não são isomorfas a produtos diretos de álgebras de Boole diretamente indecomponíveis. Assim, as álgebras diretamente indecomponíveis não podem ser consideradas como "blocos de construção" de toda a álgebra. A necessidade de obter "blocos de construção" gerais, levou Birkhoff a considerar um tipo de produto de álgebras diferente do produto direto.

Definição

Sejam $\mathcal{A}$ uma álgebra e $(\mathcal{A}_i)_{i\in I}$ uma família de álgebras do mesmo tipo. Diz-se que a álgebra $\mathcal{A}$ é um ***produto subdireto da família*** $(\mathcal{A}_i)_{i\in I}$ *se:*

(i) *$\mathcal{A}$ é uma subálgebra de $\prod_{i\in I}\mathcal{A}_i$,*

(ii) *para cada $i \in I$, $p_i(\mathcal{A}) = \mathcal{A}_i$.*

Note-se que se $I = \emptyset$, então $\mathcal{A}$ é produto subdireto de $(\mathcal{A}_i)_{i\in I}$ se e só se $\mathcal{A}$ é a álgebra trivial.

Exemplo

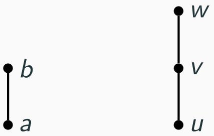
1) Sejam $(\mathcal{A}_i)_{i\in I}$ uma família de álgebras do mesmo tipo. O produto direto $\prod_{i\in I}\mathcal{A}_i$ é um produto subdireto de $(\mathcal{A}_i)_{i\in I}$.

2) Para qualquer álgebra $\mathcal{A}=(A;F)$ que não tenha operações nulárias, verifica-se facilmente que o conjunto $\triangle_A=\{(a,a)\,|\,a\in A\}$ é um subuniverso de $\mathcal{A}\times\mathcal{A}$; representemos por $\triangle_{\mathcal{A}}$ a subálgebra de $\mathcal{A}\times\mathcal{A}$ com universo $\triangle_A$. Uma vez que $p_1(\triangle_A)=p_2(\triangle_A)=A$, então $\triangle_{\mathcal{A}}$ é um produto subdireto de $(\mathcal{A}_i)_{i\in\{1,2\}}$, onde $\mathcal{A}_1=\mathcal{A}_2=\mathcal{A}$.

Elementos de álgebra universal

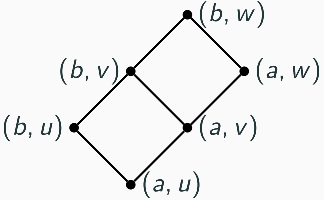
Exemplo

3) Considerando os reticulados $\mathbf{2}$ *e* $\mathbf{3}$, *i.e., as cadeias com dois e três elementos,*



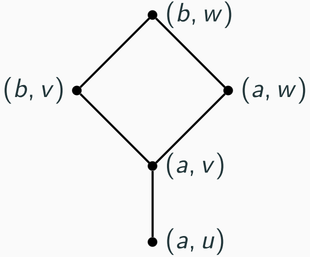
$\mathbf{2}$ $\quad\quad$ $\mathbf{3}$

o seu produto direto é o reticulado representado pelo diagrama



Exemplo

O sub-reticulado de $\mathbf{2} \times \mathbf{3}$ *representado por*



é um produto subdireto da família de álgebras $(\mathcal{A}_i)_{i \in \{1,2\}}$ *onde* $\mathcal{A}_1 = \mathbf{2}$ *e* $\mathcal{A}_2 = \mathbf{3}$.

Definição

*Sejam $\mathcal{A}$ uma álgebra e $(\mathcal{A}_i)_{i\in I}$ uma família de álgebras do mesmo tipo. A um monomorfismo $\alpha : \mathcal{A} \to \prod_{i\in I} \mathcal{A}_i$ tal que $\alpha(\mathcal{A})$ é um produto subdireto de $(\mathcal{A}_i)_{i\in I}$ dá-se a designação de **mergulho subdireto**.*

Teorema

Sejam $\mathcal{A} = (A; F)$ uma álgebra e $(\theta_i)_{i\in I}$ uma família de congruências em $\mathcal{A}$ tal que $\bigcap_{i\in I} \theta_i = \triangle_A$. Então a correspondência $\alpha : A \to \prod_{i\in I} A/\theta_i$, dada por $(\alpha(a))(i) = [a]_{\theta_i}$, para todo $a \in A$, é um mergulho subdireto.

Demonstração.

De um teorema anterior sabe-se que a correspondência α é um homomorfismo de $\mathcal{A}$ em $\prod_{i \in I} \mathcal{A}/\theta_i$.

A aplicação α também é injetiva, pois, para quaisquer $a, b \in A$,

$$\begin{array}{rcl} \alpha(a) = \alpha(b) & \Rightarrow & (\forall i \in I, [a]_{\theta_i} = [b]_{\theta_i}) \\ & \Rightarrow & (\forall i \in I, (a, b) \in \theta_i) \\ & \Rightarrow & (a, b) \in \bigcap_{i \in I} \theta_i = \triangle_A \\ & \Rightarrow & a = b. \end{array}$$

Então α é um monomorfismo.

A respeito de $\alpha(\mathcal{A})$ verifica-se facilmente que esta álgebra é um produto subdireto de $(\mathcal{A}/\theta_i)_{i \in I}$, uma vez que $\alpha(\mathcal{A}) \leq \prod_{i \in I} (\mathcal{A}/\theta_i)_{i \in I}$ e é óbvio que $p_i(\alpha(A)) = A/\theta_i$, para todo $i \in I$. $\square$

À semelhança do que sucede com o produto direto, prova-se que toda a álgebra é isomorfa a um produto subdireto de álgebras.

Teorema

Sejam $\mathcal{A} = (A; F)$ uma álgebra e $(\theta_i)_{i \in I}$ uma família de congruências em $\mathcal{A}$ tal que $\bigcap_{i \in I} \theta_i = \triangle_A$. Então $\mathcal{A}$ é isomorfa a um produto subdireto da família de álgebras $(\mathcal{A}/\theta_i)_{i \in I}$.

Demonstração.

Pelo teorema anterior sabe-se que a aplicação $\alpha : A \to \prod_{i \in I} A/\theta_i$, definida por $(\alpha(a))(i) = [a]_{\theta_i}$, para todo $a \in A$, é um monomorfismo. Logo $\mathcal{A} \cong \alpha(\mathcal{A})$. Pelo mesmo teorema sabe-se que $\alpha(\mathcal{A})$ é um produto subdireto da família de álgebras $(\mathcal{A}/\theta_i)_{i \in I}$. □

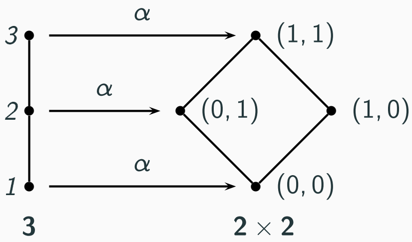
Em analogia com a definição de álgebras diretamente indecomponíveis, pretendemos considerar álgebras que não possam ser expressas como produto subdireto de álgebras mais pequenas, com excepção dos casos triviais.

Definição

Uma álgebra $\mathcal{A}$ diz-se ***subdiretamente irredutível*** *se, para qualquer família $(\mathcal{A})_{i \in I}$ de álgebras do mesmo tipo de $\mathcal{A}$ e para qualquer mergulho subdireto $\alpha : \mathcal{A} \to \prod_{i \in I} \mathcal{A}_i$, existe $i \in I$ tal que $p_i \circ \alpha$ é um isomorfismo.*

Exemplo

A cadeia com três elementos $\mathbf{3}$ *não é subdiretamente irredutível. De facto, considerando o monomorfismo* α *de* $\mathbf{3}$ *em* $\mathbf{2} \times \mathbf{2}$ *definido da forma seguinte*



verifica-se que este monomorfismo é um mergulho subdireto, pois a sua imagem $\{(0,0),(0,1),(1,1)\}$ *é um produto subdireto de* $(\mathcal{A}_i)_{i \in \{1,2\}}$*, onde* $\mathcal{A}_1 = \mathcal{A}_2 = \mathbf{2}$*, mas nem* $p_1 \circ \alpha$ *nem* $p_2 \circ \alpha$ *é um monomorfismo.*

Uma caracterização útil das álgebras subdiretamente irredutíveis e que é geralmente usada para identificar estas álgebras é dada pelo resultado seguinte.

Teorema

Uma álgebra $\mathcal{A}$ *é subdiretamente irredutível se e só se* $\mathcal{A}$ *é trivial ou* $\mathrm{Cong}(\mathcal{A}) \setminus \{\triangle_{\mathcal{A}}\}$ *tem elemento mínimo. No segundo caso, o elemento mínimo de* $\mathrm{Cong}(\mathcal{A}) \setminus \{\triangle_{\mathcal{A}}\}$ *é* $\bigcap(\mathrm{Cong}(\mathcal{A}) \setminus \{\triangle_{\mathcal{A}}\})$ *e é uma congruência principal.*

Uma álgebra diretamente indecomponível nem sempre é uma álgebra subdiretamente irredutivel (basta considerar como exemplo as cadeias com exatamente três elementos), mas o recíproco verifica-se necessariamente.

Teorema

Toda a álgebra subdiretamente irredutível é diretamente indecomponível.

Demonstração.

Do teorema anterior segue que as únicas congruências fator de uma álgebra subdiretamente irredutível $\mathcal{A} = (A; F)$ são as congruências $\triangle_A$ e ∇_A. Logo $\mathcal{A}$ é diretamente indecomponível. $\square$

Teorema (Birkhoff)
Toda a álgebra é isomorfa a um produto subdireto de álgebras subdiretamente irredutíveis.

No que se segue consideramos um tipo especial de álgebras subdiretamente irredutíveis.

Definição

*Uma álgebra $\mathcal{A}$ diz-se **simples** se* $\mathrm{Cong}(\mathcal{A}) = \{\triangle_A, \nabla_A\}$. *Uma congruência θ de $\mathcal{A}$ é maximal se o intervalo $[\theta, \nabla_A]$ tem exatamente dois elementos.*

Teorema

*Sejam $\mathcal{A}$ uma álgebra e $\theta \in \mathrm{Cong}(\mathcal{A})$. Então a álgebra $\mathcal{A}/\theta$ é simples se e só se θ é uma congruência **maximal** em $\mathcal{A}$ ou $\theta = \nabla_A$.*

Operadores e variedades

Um tema importante em álgebra universal é o estudo de classes de álgebras do mesmo tipo que sejam fechadas para a formação de subálgebras, imagens homomorfas e produtos diretos.

A uma função que associa a uma classe de álgebras (todas do mesmo tipo) uma classe de álgebras (do mesmo tipo) damos a designação de ***operador***.

Dados operadores O_1 e O_2, escreve-se $O_1 \leq O_2$ se $O_1(\mathbf{K}) \subseteq O_2(\mathbf{K})$, para qualquer classe $\mathbf{K}$ de álgebras.

Os operadores podem ser compostos dando origem a novos operadores.

Dados operadores O_1 e O_2 e uma classe $\mathbf{K}$ de álgebras, escreve-se $O_1O_2(\mathbf{K})$ em vez de $O_1(O_2(\mathbf{K}))$ e ${O_1}^2(\mathbf{K})$ em vez de $O_1(O_1(\mathbf{K}))$.

Um operador O diz-se ***idempotente*** se $O^2 = O$.

Dada uma classe **K** de álgebras do mesmo tipo, representamos por:

- $S(\mathbf{K})$ a classe de todas as subálgebras de elementos de **K**;
- $H(\mathbf{K})$ a classe de todas as imagens homomorfas de elementos de **K**;
- $I(\mathbf{K})$ a classe de todas as imagens isomorfas de elementos de **K**;
- $P(\mathbf{K})$ a classe de todos os produtos diretos de famílias não vazias de elementos de **K**;
- $P_S(\mathbf{K})$ a classe de todos os produtos subdiretos de famílias não vazias de elementos de **K**.

Para cada um dos operadores O definidos anteriormente, assumimos que $O(\emptyset) = \emptyset$ e verifica-se o seguinte:

- $\mathbf{K} \subseteq O(\mathbf{K})$, para qualquer classe $\mathbf{K}$ de álgebras do mesmo tipo;
- se $\mathbf{K}_1$ e $\mathbf{K}_2$ são classes de álgebras do mesmo tipo tais que $\mathbf{K}_1 \subseteq \mathbf{K}_2$, então $O(\mathbf{K}_1) \subseteq O(\mathbf{K}_2)$.

O resultado seguinte estabelece mais algumas propriedades a respeito destes operadores.

Teorema

Seja $\mathbf{K}$ *uma classe de álgebras. Então:*

(i)	$SH(\mathbf{K}) \subseteq HS(\mathbf{K})$;	*(ii)*	$PS(\mathbf{K}) \subseteq SP(\mathbf{K})$;	*(iii)*	$PH(\mathbf{K}) \subseteq HP(\mathbf{K})$;
(iv)	$H^2(\mathbf{K}) = H(\mathbf{K})$;	*(v)*	$I^2(\mathbf{K}) = I(\mathbf{K})$;	(vi)	$S^2(\mathbf{K}) = S(\mathbf{K})$;
(vii)	$(IP)^2(\mathbf{K}) = IP(\mathbf{K})$.				.

Demonstração:

(i) Seja $\mathcal{A} = (A; F) \in SH(\mathbf{K})$.

Então existe $\mathcal{B} \in \mathbf{K}$ e um epimorfimo $\alpha : \mathcal{B} \to \mathcal{C}$ tal que $\mathcal{A} \leq \mathcal{C}$.

Como α é sobrejetivo, então $\alpha^{\leftarrow}(A)$ é não vazio.

Seja $\alpha^{\leftarrow}(\mathcal{A})$ a álgebra pré-imagem de $\mathcal{A}$.

Uma vez que $\alpha^{\leftarrow}(\mathcal{A}) \leq \mathcal{B}$ e $\alpha(\alpha^{\leftarrow}(\mathcal{A})) = \mathcal{A}$, então $\mathcal{A} \in HS(\mathbf{K})$.

Demonstração.

(ii) Seja $\mathcal{A} = (A; F) \in PS(\mathbf{K})$. Então $\mathcal{A} = \prod_{i \in I} \mathcal{A}_i$, onde $\mathcal{A}_i \leq \mathcal{B}_i$, para algum $\mathcal{B}_i \in \mathbf{K}$. Uma vez que $\prod_{i \in I} \mathcal{A}_i \leq \prod_{i \in I} \mathcal{B}_i$, então $\mathcal{A} \in SP(\mathbf{K})$.

(iii) Seja $\mathcal{A} = (A; F) \in PH(\mathbf{K})$. Então existem álgebras $\mathcal{B}_i \in \mathbf{K}$ e epimorfismos $\alpha_i : \mathcal{B}_i \to \mathcal{A}_i$ tais que $\mathcal{A} = \prod_{i \in I} \mathcal{A}_i$. Facilmente se verifica que a aplicação $\alpha : \prod_{i \in I} \mathcal{B}_i \to \prod_{i \in I} \mathcal{A}_i$ definida por $(\alpha(b))(i) = \alpha_i(b(i))$ é um epimorfismo. Logo $\mathcal{A} \in HP(\mathbf{K})$. $\square$

Uma classe $\mathbf{K}$ de álgebras do mesmo tipo diz-se ***fechada*** para um operador O se $O(\mathbf{K}) \subseteq \mathbf{K}$.

Teorema

Seja $\mathbf{K}$ *uma classe de álgebras. Se a classe* $\mathbf{K}$ *é fechada para um operador* $O \in \{S, H, I, P, P_S\}$*, então* $O(\mathbf{K}) = \mathbf{K}$.

Definição

Seja $\mathbf{K}$ *uma classe não vazia de álgebras do mesmo tipo. Diz-se que* $\mathbf{K}$ *é uma* ***variedade*** *se é fechada para a formação de imagens homomorfas, subálgebras e produtos diretos.*

Uma vez que a interseção de uma familia não vazia de variedades de álgebras do mesmo tipo é uma variedade e atendendo a que a classe formada por todas as álgebras do mesmo tipo é uma variedade, conclui-se que para qualquer classe $\mathbf{K}$ de álgebras do mesmo tipo existe a menor variedade que contém $\mathbf{K}$.

Definição

Seja $\mathbf{K}$ *uma classe de álgebras do mesmo tipo. Designa-se por* ***variedade gerada por*** $\mathbf{K}$*, e representa-se por* $V(\mathbf{K})$*, a menor variedade que contém* $\mathbf{K}$.

Teorema (Teorema de Tarski)

Seja $\mathbf{K}$ *uma classe de álgebras do mesmo tipo. Então* $V(\mathbf{K}) = HSP(\mathbf{K})$.

Demonstração.

Por um lado, como $\mathbf{K} \subseteq V(\mathbf{K})$ e $V(\mathbf{K})$ é uma variedade, tem-se

$$HSP(\mathbf{K}) \subseteq HSP(V(\mathbf{K})) = HS(V(\mathbf{K})) = HV(\mathbf{K}) = V(\mathbf{K}).$$

Por outro lado, tem-se

$$\begin{aligned}
&HHSP(\mathbf{K}) = HSP(\mathbf{K}) \\
&SHSP(\mathbf{K}) \subseteq HSSP(\mathbf{K}) = HSP(\mathbf{K}); \\
&PHSP(\mathbf{K}) \subseteq HPSP(\mathbf{K}) \subseteq HSPP(\mathbf{K}) \subseteq HSIPIP(\mathbf{K}) \\
&\qquad\qquad \subseteq HSIP(\mathbf{K}) \subseteq HSHP(\mathbf{K}) \subseteq HHSP(\mathbf{K}) = HSP(\mathbf{K}).
\end{aligned}$$

Logo $HSP(\mathbf{K})$ é uma variedade. Por conseguinte, atendendo a que $\mathbf{K} \subseteq HSP(\mathbf{K})$, tem-se $V(\mathbf{K}) \subseteq HSP(\mathbf{K})$. □

O resultado seguinte é bastante útil no estudo de variedades.

Teorema

Seja $\mathbf{K}$ *uma variedade. Então toda a álgebra de* $\mathbf{K}$ *é isomorfa a um produto subdireto de álgebras subdiretamente irredutíveis de* $\mathbf{K}$*.*

Como consequência imediata deste teorema tem-se o resultado seguinte.

Corolário

Toda a variedade é gerada pelas suas álgebras subdiretamente irredutíveis.

Álgebras livres, Termos, Identidades, Teorema de Birkhoff

Nas secções anteriores foram abordados alguns processos algébricos para a construção de álgebras e foi dada especial atenção ao estudo de classes de álgebras que são fechadas para alguns desses processos de construção, mais especificamente, estudaram-se classes fechadas para a formação de subálgebras, para a formação de imagens homomorfas e para a formação de produtos diretos. Considerando que a maioria das álgebras que se estudam são definidas por operações que satisfazem determinadas identidades, é importante averiguar se os processos de construção referidos anteriormente também preservam as identidades que são satisfeitas pelas álgebras de uma determinada classe.

No sentido de fazer tal estudo, nesta secção começamos por introduzir os conceitos de termo e de álgebras livres, conceitos estes que serão posteriormente utilizados para definir identidades e estabelecer a ligação existente entre a abordagem algébrica e a abordagem equacional adotada no estudo das álgebras.

Álgebras livres

Definição

Sejam $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ), $\mathcal{U} = (U; F)$ *uma álgebra de tipo* (O, τ) *e* X *um subconjunto de* U. *Diz-se que a álgebra* $\mathcal{U}$ *é* ***livre para*** $\mathbf{K}$ ***sobre*** X *se:*

(i) $\mathcal{U}$ *é gerada por* X*;*

(ii) *para cada álgebra* $\mathcal{A} \in \mathbf{K}$ *e para cada aplicação* $\alpha : X \to A$, *existe um homomorfismo* $\overline{\alpha} : \mathcal{U} \to \mathcal{A}$ *que estende* α *(i.e.,* $\overline{\alpha}(x) = \alpha(x)$, *para todo* $x \in X$*).*

O conjunto X *diz-se um conjunto de* ***geradores livres*** *de* $\mathcal{U}$ *e a álgebra* $\mathcal{U}$ *diz-se* ***livremente gerada por*** X***.***

Lema

Sejam $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ)*,* $\mathcal{U} = (U; F)$ *uma álgebra de tipo* (O, τ) *e* X *um subconjunto de* U*. Se a álgebra* $\mathcal{U}$ *é livre para* $\mathbf{K}$ *sobre* X*, então, para qualquer álgebra* $\mathcal{A} = (A; G) \in \mathbf{K}$ *e para qualquer aplicação* $\alpha : X \to A$*, existe um único homomorfismo* $\overline{\alpha} : \mathcal{U} \to \mathcal{A}$ *que estende* α*.*

Demonstração.

A existência de $\overline{\alpha}$ é garantida pelo facto de $\mathcal{U}$ ser livre para $\mathbf{K}$ sobre X. A unicidade de $\overline{\alpha}$ resulta de $\mathcal{U}$ ser gerada por X. $\square$

Teorema

Sejam $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ), $\mathcal{U}_1 = (U_1; F)$, $\mathcal{U}_2 = (U_2; G)$ *álgebras de* $\mathbf{K}$ *e* X *e* Y *subconjuntos de* U_1 *e* U_2*, respetivamente. Se* $\mathcal{U}_1$ *e* $\mathcal{U}_2$ *são álgebras livres para* $\mathbf{K}$ *sobre* X *e* Y*, respetivamente, e* $|X| = |Y|$*, então* $\mathcal{U}_1 \cong \mathcal{U}_2$.

Termos

Definição

*Sejam (O, τ) um tipo algébrico e X um conjunto tal que $X \cap O = \emptyset$. Aos objetos de X dá-se a designação de **variáveis**. O **conjunto** $T(X)$ **dos termos de tipo** (O, τ) **sobre** X é o menor conjunto tal que:*

(i) $X \cup O_0 \subseteq T(X)$.

(ii) *Se* $(t_1, \ldots, t_k) \in (T(X))^k$ *e* f *é um símbolo de operação de* O *de aridade* k*, onde* $k \in \mathbb{N}$*, então* $f(t_1, \ldots, t_k) \in T(X)$.

Note-se que $T(X) \neq \emptyset$ se e só se $X \cup O_0 \neq \emptyset$.

Para um símbolo de operação binário $\cdot$ é usual adotar a notação $t_1 \cdot t_2$, em vez de $\cdot(t_1, t_2)$.

Dado $t \in T(X)$, escreve-se $t(x_1, \ldots, x_n)$ para indicar que as variáveis que ocorrem no termo t pertencem a $\{x_1, \ldots, x_n\}$.

Um termo t diz-se n-ário se o número de variáveis que ocorrem em t é menor ou igual a n.

Exemplo

(1) Sejam $X = \{x, y, z\}$ *e* (O, τ) *um tipo algébrico, onde* O *é constituído por dois símbolos de operação binários* $\cdot$ *e* $+$*. Então*

$$x,\ y,\ z,\ x \cdot (y + z),\ (x \cdot y) + (x \cdot z)$$

são alguns dos termos sobre X*.*

(2) Sejam $X = \{x\}$ *e* (O, τ) *o tipo algébrico onde* $O = \{+, \cdot, -\} \cup \{r\}_{r \in \mathbb{R}}$ *e* $\tau : O \to \mathbb{N}_0$ *é definida por* $\tau(+) = \tau(\cdot) = \tau(-) = 2$ *e* $\tau(r) = 0$*, para cada* $r \in \mathbb{R}$*. Então o conjunto dos termos de tipo* (O, τ) *sobre* X *é*

$$R[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in \mathbb{R}, i \in \mathbb{N}_0\}.$$

Definição

*Sejam (O, τ) um tipo algébrico, X um conjunto tal que $X \cap O = \emptyset$, $X \cup O_0 \neq \emptyset$. Dado um termo n-ário $t(x_1, \ldots, x_n) \in T(X)$, $n \in \mathbb{N}$, e dada uma álgebra $\mathcal{A} = (A; F)$ de tipo (O, τ), define-se a função $t^{\mathcal{A}} : A^n \to A$, designada por **função termo em $\mathcal{A}$ induzida por** t, da seguinte forma:*

(1) se t é uma variável x_i, então

$$t^{\mathcal{A}}(a_1, \ldots, a_n) = a_i,$$

para qualquer $(a_1, \ldots, a_n) \in A^n$.

(2) se t é da forma $f(t_1(x_1, \ldots, x_n), \ldots, t_k(x_1, \ldots, x_n))$, onde f é um símbolo de operação de O de aridade k, $k \in \mathbb{N}_0$, e $t_1^{\mathcal{A}}$, ..., $t_k^{\mathcal{A}}$ são as funções termo em $\mathcal{A}$ induzidas pelos termos n-ários $t_1, \ldots, t_k \in T(X)$, então

$$t^{\mathcal{A}}(a_1, \ldots, a_n) = f^{\mathcal{A}}({t_1}^{\mathcal{A}}(a_1, \ldots, a_n), \ldots, {t_k}^{\mathcal{A}}(a_1, \ldots, a_n)),$$

para quaisquer $(a_1, \ldots, a_n) \in A^n$.

O resultado seguinte estabelece algumas propriedades importantes relativas a funções termo, mais especificamente, estabelece que as funções termo se comportam de forma análoga às operações fundamentais de uma álgebra no que respeita a congruências e a homomorfismos.

Teorema

Sejam $\mathcal{A} = (A; F)$ uma álgebra de tipo (O, τ), X um conjunto tal que $X \cap O = \emptyset$ e $X \cup O_0 \neq \emptyset$, $n \in \mathbb{N}$ e $t^{\mathcal{A}}$ a função termo em $\mathcal{A}$ induzida por um termo n-ário $t \in T(X)$.

(i) *Se $\mathcal{B} = (B; G)$ é uma subálgebra de $\mathcal{A}$, então $t^{\mathcal{A}}(b_1, \ldots, b_n) \in B$, para quaisquer $b_1, \ldots, b_n \in B$.*

(ii) *Se $\theta \in \operatorname{Con} \mathcal{A}$ e $(a_i, b_i) \in \theta$, para qualquer $i \in \{1, \ldots, n\}$, então*

$$t^{\mathcal{A}}(a_1, \ldots, a_n) \, \theta \, t^{\mathcal{A}}(b_1, \ldots, b_n).$$

(iii) *Se $\mathcal{B} = (B; G)$ é uma álgebra de tipo (O, τ) e $\alpha : \mathcal{A} \to \mathcal{B}$ é um homomorfismo, então*

$$\alpha(t^{\mathcal{A}}(a_1, \ldots, a_n)) = t^{\mathcal{B}}(\alpha(a_1), \ldots, \alpha(a_n)),$$

para qualquer $(a_1, \ldots, a_n) \in A^n$.

Dado um tipo algébrico (O, τ) e um conjunto X, define-se de forma natural uma álgebra de tipo (O, τ) que tem como universo o conjunto de termos $T(X)$.

Definição

*Sejam (O, τ) um tipo algébrico e X um conjunto tal que $X \cap O = \emptyset$ e $X \cup O_0 \neq \emptyset$. Designa-se por **álgebra dos termos de tipo (O, τ) sobre** X, e representa-se por $\mathcal{T}(X)$, a álgebra $\mathcal{T}(X) = (T(X); (f^{\mathcal{T}(X)})_{f \in O})$ onde, para qualquer símbolo de operação $f \in O$ de aridade k, $k \in \mathbb{N}_0$, $f^{\mathcal{T}(X)} : T(X)^k \to T(X)$ é a operação definida por*

$$f^{\mathcal{T}(X)}(t_1, \ldots, t_k) = f(t_1, \ldots, t_k),$$

para qualquer $(t_1, \ldots, t_k) \in (T(X))^k$.

Claramente, a álgebra $\mathcal{T}(X)$ é gerada por X.

Teorema

Sejam (O, τ) um tipo algébrico, $\mathbf{K}_{(O,\tau)}$ a classe de todas as álgebras de tipo (O, τ) e X um conjunto tal que $X \cap O = \emptyset$ e $X \cup O_0 \neq \emptyset$. Então a álgebra $\mathcal{T}(X)$ é livre para $\mathbf{K}_{(O,\tau)}$ sobre X.

Demonstração.

Já foi observado anteriormente que X gera $\mathcal{T}(X)$. Também se prova que, para cada álgebra $\mathcal{A} = (A; F) \in \mathbf{K}_{(O,\tau)}$ e para cada função $\alpha : X \to A$, existe um homomorfismo $\overline{\alpha} : \mathcal{T}(X) \to \mathcal{A}$ que estende α. De facto, é simples verificar que a aplicação $\overline{\alpha} : T(X) \to A$ definida recursivamente por

(i) $\overline{\alpha}(x) = \alpha(x)$, para todo $x \in X$,

(ii) $\overline{\alpha}(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\overline{\alpha}(t_1), \ldots, \overline{\alpha}(t_n))$, para quaisquer $t_1, \ldots, t_n \in T(X)$ e $f \in O_n$,

é um homomorfismo de $\mathcal{T}(X)$ em $\mathcal{A}$ que estende α. □

Corolário

Sejam (O, τ) *um tipo algébrico,* $\mathbf{K}$ *uma classe de álgebras de tipo* (O, τ) *e* X *um conjunto tal que* $X \cap O = \emptyset$ *e* $X \cup O_0 \neq \emptyset$*. Então a álgebra* $\mathcal{T}(X)$ *é livre para* $\mathbf{K}$ *sobre* X*.*

Identidades, Teorema de Birkhoff

Um dos mais conhecidos teoremas de Birkhoff estabelece que as classes de álgebras definidas por identidades são precisamente as classes de álgebras que são fechadas para a formação de imagens homomorfas, subálgebras e produtos diretos. Nesta secção estudamos identidades e a sua relação com álgebras livres, no sentido de se estabelecer o referido teorema.

Definição

Sejam (O, τ) *um tipo algébrico e* X *um conjunto de variáveis tal que* $X \cap O = \emptyset$. *Uma* ***identidade de tipo*** (O, τ) ***sobre*** X *é uma expressão da forma*

$$p \approx q,$$

onde $p, q \in T(X)$. *Representa-se por* $\mathrm{Id}(X)$ *o conjunto de todas as identidades de tipo* (O, τ) *sobre* X.

Definição (continuação)

Dada uma álgebra $\mathcal{A}$ de tipo (O, τ), diz-se que ***a álgebra*** $\mathcal{A}$ ***satisfaz a identidade***

$$p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$$

se, para quaisquer $a_1, \ldots, a_n \in A$,

$$p^{\mathcal{A}}(a_1, \ldots, a_n) = q^{\mathcal{A}}(a_1, \ldots, a_n).$$

Neste caso, diz-se que a identidade ***é verdadeira em*** $\mathcal{A}$ *ou que se* ***verifica em*** $\mathcal{A}$*, e escreve-se*

$$A \models p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$$

ou, mais abreviadamente,

$$A \models p \approx q.$$

Definição (continuação)

Se Σ é um conjunto de identidades, diz-se que $\mathcal{A}$ ***satisfaz*** *Σ, e escreve-se*

$$A \models \Sigma,$$

se $A \models p \approx q$, para qualquer $p \approx q \in \Sigma$.

Uma classe de álgebras $\mathbf{K}$ ***satisfaz uma identidade*** *$p \approx q$, e escreve-se*

$$\mathbf{K} \models p \approx q,$$

se cada uma das álgebras de $\mathbf{K}$ satisfaz $p \approx q$. Diz-se que $\mathbf{K}$ ***satisfaz um conjunto de identidades*** *Σ, e escreve-se*

$$\mathbf{K} \models \Sigma,$$

se $\mathbf{K}$ satisfaz cada uma das identidades de Σ.

Definição (continuação)

O conjunto de todas as identidades de tipo (O, τ) *sobre* X *que são satisfeitas por* $\mathbf{K}$ *é representado por* $\mathrm{Id}_{\mathbf{K}}(X)$*; i.e.,*

$$\mathrm{Id}_{\mathbf{K}}(X) = \{p \approx q \in \mathrm{Id}(X) : \mathbf{K} \models p \approx q\}.$$

Lema

Para qualquer classe $\mathbf{K}$ *de álgebras de tipo* (O, τ), *as classes* $\mathbf{K}$, $I(\mathbf{K})$, $S(\mathbf{K})$, $H(\mathbf{K})$, $P(\mathbf{K})$ *e* $HSP(\mathbf{K})$ *satisfazem as mesmas identidades sobre qualquer conjunto de variáveis* X.

Definição

Dado um conjunto Σ de identidades de tipo (O, τ), define-se $M(\Sigma)$ como sendo a classe de todas as álgebras de tipo (O, τ) que satisfazem Σ.
*Uma classe $\mathbf{K}$ de álgebras de tipo (O, τ) diz-se uma **classe equacional** se existe um conjunto de identidades Σ tal que $\mathbf{K} = M(\Sigma)$. Neste caso, diz-se que a classe $\mathbf{K}$ é **definida** ou **axiomatizada** por Σ.*

Teorema (Birkhoff)

Seja $\mathbf{K}$ uma classe de álgebras de tipo (O, τ). Então $\mathbf{K}$ é uma classe equacional se e só se $\mathbf{K}$ é uma variedade.

Exemplo

- *Semigrupos: A classe* **S** *dos semigrupos é uma variedade;*

$$\mathbf{S} = M(\{x(yz) \approx (xy)z\}).$$

- *Grupos: A classe* **G** *dos grupos vistos como álgebras de tipo (2,1,0) é uma variedade;*

$$\mathbf{G} = M(\{x(yz) \approx (xy)z, x1_{\mathbf{G}} \approx 1_{\mathbf{G}}x \approx x, xx^{-1} \approx x^{-1}x \approx 1_{\mathbf{G}}\}).$$

A classe dos grupos vistos como álgebras do tipo (2) não é uma variedade.

Exemplo

- *Reticulados: A classe* **R** *dos reticulados é uma variedade;*

$$\begin{aligned}\mathbf{R} \quad = M(\{ & x \wedge y \approx y \wedge x, x \vee y \approx y \vee x, \\ & x \wedge (y \wedge z) \approx (x \wedge y) \wedge z, x \vee (y \vee z) \approx (x \vee y) \vee z, \\ & x \vee (x \wedge y) \approx x, x \wedge (x \vee y) \approx x\}).\end{aligned}$$