Estudos do I.S.C.A.A II Série • Nº 3 e 4 • 1997/98
Revista de Publicação Anual

Direcção: Joaquim José da Cunha

Coordenação: José Fernandes de Sousa
Vírginia Maria Granate Costa e Sousa

Conselho Consultivo: Professores Coordenadores das Áreas Científicas do I.S.C.A.A.

Edição e Propriedade: Instituto Superior de Contabilidade e Administração de Aveiro

Apoio Administrativo e Assinaturas: Biblioteca do I.S.C.A.A.
R. Associação Humanitária dos Bombeiros Velhos de Aveiro
Apartado 58 - 3811/953 - Aveiro
Tel.: (034) 381977 - 381911; Fax: (034) 28975

Preço: 1.500$00

ISSN: 0873-2019

Depósito legal nº: 922 54/95
Capa: Design. Francisco Espindola
Trat. de texto: apoio técnico de Maximina Gonçalves Marieiro
Impressão: Tipografia Minerva Central, Lda./1998

EXTENSÕES DE UM ANEL.
CORPO DE QUOCIENTES Q.

MARGARIDA MARIA SOLTEIRO MARTINS PINHEIRO
Professora Adjunta de Matemática
I.S.C.A.A.

SUMÁRIO

O presente artigo faz parte de um dos temas discutidos no concurso de provas públicas para Professores-Adjuntos do Ensino Superior Politécnico, realizado em Dezembro de 1994. Após a introdução de alguns conceitos básicos, provam-se dois resultados sobre extensões de um anel.

No primeiro, mostra-se que a partir de um anel sem identidade é possível construir um anel com identidade que contem um subanel isomorfo ao primeiro.

No segundo resultado, mostra-se que a partir de qualquer domínio de integridade é possível construir um corpo que contem uma cópia isomorfa ao domínio inicial.

PRELIMINARES

Comecemos por introduzir alguns conceitos.

Definição 1

Chama-se anel a todo o termo (E,θ,*) onde E é um conjunto não vazio e θ e * são duas operações internas em E tais que:

(E,θ) é grupo abeliano e (E,*) é semi-grupo e * é distributiva em relação a θ; isto é,

$$\forall a,b,c \in E, a * (b\theta c) = (a * b)\theta(a * c)$$

$$\forall a,b,c \in E, (a\theta b) * c = (a * c)\theta(b * c)$$

Ao elemento neutro de θ chamamos zero do anel e representamos por 0 [1].

Definição 2

Um anel E diz-se comutativo se a multiplicação é comutativa.

Definição 3

Um anel E diz-se anel unitário ou anel com identidade se a multiplicação tem elemento neutro [2].

---

[1] Também podemos definir anel de outro modo: um anel é um conjunto E não vazio, munido de duas operações, uma chamada adição e usualmente denotada por + e outra chamada multiplicação e usualmente notada por . (ou ausência de ponto) tais que:

(E,+) é grupo abeliano, (E,.) é semi-grupo e a multiplicação é distributiva relativamente à adição; isto é

$$\forall a,b,c \in E, a(b+c) = ab + ac$$

$$\forall a,b,c \in E, (a+b)c = ac + bc$$

De agora em diante e supondo que não haja perigo de confusão, denotaremos o anel (E,+,.) simplesmente por E.

[2] O elemento neutro da multiplicação, caso exista, será denotado por 1 e diz-se identidade ou elemento unidade do anel.

Definição 4
Seja (E,+,.) um anel e S um subconjunto de E.
Diz-se que S é <u>subanel</u> de E se S é um anel para as operações que conferem a E a estrutura de anel.

Proposição 1
Seja E um anel. Então:
i) $\forall r \in E, r0 = 0r = 0$
ii) $\forall r, s \in E, (-r)s = r(-s) = -(rs)$
iii) $\forall r, s \in E, (-r)(-s) = rs$

Demonstração:
I) Como 0 é o elemento neutro da adição, 0+0=0 e portanto $r(0+0) = r0$. Atendendo à distribuitividade do anel vem, $r0 + r0 = r0$. Pela lei do corte, válida em E, conclui-se que $r0 = 0$. Provámos então que $r0 = 0$. De modo análogo provamos que $0r = 0$. Então i) está provado.
ii) Sejam $r, s \in E$. Pretendemos mostrar, em primeiro lugar, que $(-r)s = -(rs)$. Sabemos que $r + (-r) = 0$. Atendendo à distribuitividade do anel e a i) deduz-se que
$(r + (-r))s = 0s \Leftrightarrow rs + (-r)s = 0$
Donde se conclui que $(-r)s = -(rs)$.
De modo análogo provamos que $r(-s) = -(rs)$ e portanto ii) fica provada.
iii) De ii) resulta
$(-r)(-s) = -(r(-s)) = -(-(rs)) = rs$
porque, num grupo aditivo $-(-x) = x$. Então iii) fica demonstrada.

Definição 5
Seja E um anel comutativo.
$r \in E$ diz-se um <u>divisor de zero</u> se $r \neq 0$ e existe $s \neq 0$, com $s \in E$ tal que $rs = 0$.

Definição 6
Chama-se domínio de integridade (ou simplesmente domínio) a um anel comutativo com elemento unidade (diferente do zero do anel) e sem divisores de zero.

Definição 7
Seja D um domínio de integridade e seja D' um subconjunto de D. Diz-se que D' é um subdomínio de D se e só se:
i) D' é subanel de D;
ii) D' contem a identidade;
iii) D' não tem divisores de zero.

Definição 8
Seja D um domínio de integridade e $a \in D \setminus \{0\}$.
Diz-se que a é cancelável à esquerda se, $\forall x, y \in D, ax = ay \Rightarrow x = y$

Proposição 2
Seja E um domínio de integridade. Então todo o elemento não nulo de E é cancelável em (E,.).

Demonstração:
Seja $a \in D \setminus \{0\}$. Como por hipótese D é domínio de integridade, D já é um anel comutativo pelo que basta provar que a é cancelável à esquerda. Sejam ainda $x, y \in D$ tais que $ax = ay$. Queremos provar que $x = y$. Ora
$ax = ay \Leftrightarrow ax - ay = 0 \Leftrightarrow a(x - y) = 0$
Como $a \neq 0$ e D não tem divisores de zero, tem que ser $x - y = 0$ e logo $x = y$, como pretendíamos. ♣

Proposição 3
Um subconjunto S não vazio de um anel E é um subanel se e só se:
i) Para todos $a, b \in S$, temos $a - b \in S$

ii) Para todos $a,b \in S$, temos $ab \in S$

Demonstração:

($\Rightarrow$)

Por hipótese S é um subanel de E, de onde, atendendo à definição 4 facilmente se conclui que, para todo $a,b \in S$, $a\text{-}b \in S$ e $a.b \in S$.

($\Leftarrow$)

Seja S um subconjunto não vazio de E. De i) resulta que (S,+) é um subgrupo de (E,+) e como (E,+) é grupo comutativo concluímos que (S,+) é grupo comutativo.

De ii) resulta que (.) é uma operação interna em S. Uma vez que a associatividade é uma propriedade hereditária, podemos concluir que (S,.) é semi-grupo. Analogamente, como a propriedade distributiva também é hereditária, podemos concluir que S é anel. Logo S é subanel de E, c.q.d. ♣

Definição 9

Chama-se <u>corpo</u> a todo o anel comutativo tal que o conjunto dos elementos não nulos é grupo para a multiplicação.

Provemos agora o seguinte Teorema.

Teorema 1

Seja D um domínio de integridade com um número finito de elementos. Então D é um corpo.

Demonstração:

Seja $D = \{a_1, a_2, \ldots, a_n\}$ e vamos supor, sem perda de generalidade, que os elementos estão ordenados de forma a que a_1 seja o zero do anel e a_2 seja o elemento unidade. Uma vez que D é um anel comutativo com elemento unidade, para provar que D é um corpo, falta provar que todos os elementos não nulos constituem um grupo para a multiplicação. Como, por hipótese (D,.) já é semi-grupo, só resta provar que qualquer elemento não nulo admite inverso para a multiplicação.

Seja $a_j \in D$ com $a_j \neq a_1$. Consideremos os produtos $a_j a_i$ com $i=1,...,n$. Em particular e atendendo às definições feitas tem-se $a_j a_1 = a_1$ e $a_j a_2 = a_j$. Por outro lado, atendendo à Proposição 1, se $a_i \neq a_k$ então $a_j a_i \neq a_j a_k$. Consideremos o conjunto

$$\{a_j a_1, a_j a_2, a_j a_3, \ldots, a_j a_n\} = \{a_1, a_j, a_j a_3, \ldots, a_j a_n\} = D$$

Logo, existe $a_k \in D \setminus \{a_1\}$ tal que $a_j a_k = a_2$. Como D é comutativo $a_K a_J = a_2$ e logo $a_k = (a_j)^{-1}$ o que completa a demonstração. ♣

De acordo com o teorema acabado de demonstrar, se D é um domínio de integridade finito,então D é corpo.
Mas podemos ainda dizer mais. Contudo e antes de passar ao teorema seguinte, introduzamos alguns novos conceitos.

Definição 10
Seja E um conjunto.
Chama-se relação binária definida em E a todo o subconjunto não vazio do produto cartesiano ExE=E^2

Definição 11
Seja $R \subset E^2$ uma relação binária definida em E. Diz-se que R é uma relação de equivalência se R é simultaneamente reflexiva, simétrica e transitiva.
i) R é reflexiva se para todo o $x \in E$, se tem $(x,x) \in R$.
ii) R é simétrica se para todos $x,y \in E$, se $(x,y) \in R$ então $(y,x) \in R$.
iii) R é transitiva se para todos $x,y,z \in E$, se $(x,y) \in R$ e $(y,z) \in R$ então $(x,z) \in R$.[3]

Definição 12
Seja R uma relação de equivalência sobre E e $x \in$ E.

[3] Se $(a, b) \in R$ também se pode escrever aRb.

Chama-se <u>classe de equivalência</u> de R relativa a x, ao conjunto de todos os elementos de E, R-equivalentes a x e representa-se por $\bar{x}$.

Da definição conclui-se que $\bar{x} = \{a \in E: aRx\}$.

Definição 13
Seja R uma relação de equivalência sobre E.
Ao conjunto de todas as classes de equivalência determinadas em E por R, chama-se <u>conjunto quociente</u> de E por R e nota-se por E/R.

Tem-se então que $E / R = \{\bar{x}: x \in E\}$.

Definição 14
Chama-se <u>homomorfismo</u> do anel E no anel E' a toda a aplicação φ:E→E' tal que
$\forall r, r' \in E, \varphi(r + r') = \varphi(r) + \varphi(r')$
$\forall r, r' \in E, \varphi(rr') = \varphi(r).\varphi(r')$
Se φ é ainda bijectiva, então diz-se um <u>isomorfismo</u> de E sobre E'.

EXTENSÃO DE UM ANEL SEM IDENTIDADE A UM ANEL COM IDENTIDADE

Apesar de um anel não ter necessáriamente identidade, por exemplo o anel $(Z_2,+,.)$, vamos ver que podemos sempre estender um anel sem identidade a um anel com identidade.

Teorema 2
Seja E um anel sem identidade. Então existe um anel A com identidade que contem um subanel isomorfo a E.

Demonstração:
Seja A=ExZ, onde Z designa o anel dos inteiros relativos. Em A definem-se as seguintes operações:
uma adição
$+: A....x....A......\rightarrow....A$

$$((a,m),(a',m')) \rightarrow (a,m)+(a',m') = (a+a',m+m')$$

e uma multiplicação
$..: A....x....A......\rightarrow....A$

$$((a,m),(a',m')) \rightarrow (a,m)(a',m') = (aa'+ma'+m'a,mm')$$

Vamos ver que, com estas duas operações A é um anel cujo zero é (0,0) e cuja identidade é (0,1).
Que a operação + é interna em A e que goza das propriedades comutativa e associativa, é imediato, pelas próprias definições e construção de A.
Como, para qualquer elemento (a,m) de A se tem

$$(a,m)+(0,0) = (a+0,m+0) = (a,m)$$

e para qualquer elemento (a,m) de A existe $(-a,-m)$ tal que

$$(a,m)+(-a,-m) = (a+(-a),m+(-m)) = (0,0)$$

então (A,+) é grupo comutativo.
Como (A,.) é grupoide, para garantir que (A,+,.) é anel, basta garantir que:

1) $\forall(a,m),(a',m'),(a'',m'')\in A,((a,m)(a',m'))(a'',m'')=$
$=(a,m)((a',m')(a'',m''))$

2) $\forall(a,m),(a',m'),(a'',m'')\in A,((a,m)+(a',m'))(a'',m'')=$
$=(a,m)(a'',m'')+(a',m')(a'',m'')$

$\forall(a,m),(a',m'),(a'',m'')\in A,(a,m)((a',m')+(a'',m''))=$
$=(a,m)(a',m')+(a,m)(a'',m'')$

Ora 1) e2) resultam imediatamente, efectuando os cálculos.

3) $\forall(a,m)\in A,(a,m)(0,1)=(0,1)(a,m)=(a,m)$

De facto
$(a,m)(0,1)=(0+m0+a,m)=(a,m)$ e
$(0,1)(a,m)=(0+a+m0,m)=(a,m)$
Provámos então que A um anel com identidade.

Falta provar ainda que o A contem um subanel isomorfo a E.
Seja $A'=Ex\{0\}=\{(a,0),a\in E\}\subset ExZ$. Então A' é um subanel de A.
Como $(0_E,0)\in A'$ resulta que A é não vazio.
Sejam $(a,0),(a',0)\in A'$. Então
$(a,0)-(a',0)=(a-a',0)\in A'$
$(a,0)(a',0)=(aa'+0a'+0a,0)=(aa',0)\in A'$
Logo, pela proposição 3 concluímos que A' é subanel de A.

Falta provar que tal subanel é isomorfo a E.
Considere-se a aplicação
$\varphi: E\rightarrow Ex\{0\}=A'$
$..a\rightarrow(a,0)$
É óbvio que φ é bijectiva.

Vamos provar que φ é um homomorfismo de anéis.
Sejam $a,a'\in E$. Então,
$\varphi(a+a')=(a+a',0)=(a,0)+(a',0)=\varphi(a)+\varphi(a')$

e

$$\varphi(aa') = (aa',0) = (aa'+0a'+0a,0) = (a,0)(a',0) = \varphi(a)\varphi(a')$$

o que prova que φ é um isomorfismo de anéis.
Concluímos então que A=ExZ é um anel com identidade que contem um subanel Ex{0} isomorfo a E. ♣

CONSTRUÇÃO DO CORPO DE QUOCIENTES

Que todo o corpo é anel é uma afirmação clara que resulta da própria definição.
A questão que queremos aqui colocar é a inversa: "Será que um anel arbitrário se pode estender a um corpo?"

Suponhamos E um anel comutativo com elemento unidade. Repare-se que, se E tem divisores de zero, então existem elementos não invertíveis e, pela definição 9, E não pode estender-se a um corpo. Então, para estendermos um anel E a um corpo, a primeira exigência a fazer é que E seja um domínio de integridade.

Estamos agora em condições de garantirmos que um qualquer domínio de integridade pode ser estendido a um corpo. As considerações que vamos a seguir fazer, permitem-nos, a partir de um domínio de integridade, construir um corpo, que contém esse domínio de integridade.

Teorema 3
Seja D um domínio de integridade. Então existe um corpo Q que contém um subdomínio isomorfo a D.
A esse corpo chamamos corpo das fracções ou corpo dos quocientes de D.

Demonstração:
Consideremos o produto cartesiano DxD^* onde $D^* = D \setminus \{0\}$. Em D^* vamos definir a relação binária "~" tal que *(a,b)~(c,d)* se e só se *ad=bc*. Facilmente se vê que a relação binária assim definida é uma relação de equivalência. Sendo a reflexividade e a simetria evidentes, vamos apenas provar a transitividade. Sejam então *(a,b), (c,d), (e,f)* elementos do produto cartesiano DxD^* tais que *(a,b)~(c,d)* e *(c,d)~(e,f)* . Mas então *ad=bc* e *cf=de* . Multiplicando ambos os membros de cada igualdade por *f* e *b*, respectivamente (supostos não nulos por construção) , vem *adf=bcf* e *cfb=deb* . donde concluímos que *adf=deb* , ou seja, *afd=ebd*. Atendendo agora à proposição 2, temos que *af=eb* (*d* é não nulo, por construção) . Ou seja, *(a,b)~(e,f)* . Consideremos agora o conjunto quociente $DxD^*/_{\approx}$ e notemos por $\frac{a}{b}$ a classe de equivalência que contem o elemento *(a,b)* . Ou seja, $DxD^*/_{\approx} = \{\frac{a}{b}, a \in D, b \in D^*\}$. Para simplificar, designemos por Q o conjunto quociente considerado; isto é $Q = \{\frac{a}{b}, a \in D, b \in D^*\}$. Em Q vamos definir duas operações:

i) uma adição
$QxQ \rightarrow Q$
$$(\frac{a}{b},\frac{c}{d}) \rightarrow \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

ii) uma multiplicação
$QxQ \rightarrow Q$
$$(\frac{a}{b},\frac{c}{d}) \rightarrow \frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$$

Antes de mais, comecemos por verificar que as operações assim definidas são compatíveis com a relação de equivalência "~" atrás definida. Temos então de provar que:

i) para a adição

$(a,b) \sim (a',b') \wedge (c,d) \sim (c',d') \Rightarrow (ad+bc,bd) \sim (a'd'+b'c',b'd')$

Ou seja, $\frac{a}{b} = \frac{a'}{b'} \wedge \frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$

ii) para a multiplicação

$(a,b) \sim (a',b') \wedge (c,d) \sim (c',d') \Rightarrow (ac,bd) \sim (a'c',b'd')$

Ou seja, $\frac{a}{b} = \frac{a'}{b'} \wedge \frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$

Vamos verificar a compatibilidade da adição com a relação de equivalência.

i)Sejam então $(a,b),(a',b'),(c,d),(c',d') \in DxD^*$ tais que $(a,b) \sim (a',b') \wedge (c,d) \sim (c',d')$. Ou seja, $ab' = ba'$ e $cd' = dc'$

Queremos provar que $(ad+bc)b'd' = (a'd'+b'c')bd$. Ora, atendendo a que D é domínio de integridade,

$(ad+bc)b'd' = adb'd' + bcb'd' = ab'dd' + bcd'b' = ba'dd' + bdc'b' =$

$= (a'd'+b'c')bd$

como pretendíamos.

Vamos agora verificar a compatibilidade da multiplicação com a relação de equivalência.

ii) Sejam então $(a,b),(a',b'),(c,d),(c',d') \in DxD^*$ tais que $(a,b) \sim (a',b') \wedge (c,d) \sim (c',d')$; ou seja, $ab' = ba'$ e $cd' = dc'$. Queremos provar que $acb'd' = a'c'bd$. Ora, atendendo a que D é domínio de integridade, $acb'd' = ab'cd' = ba'dc' = a'c'bd$, como pretendíamos.

Facilmente se prova que , com as operações atrás definidas, Q é um corpo cujo zero é $\frac{0}{1}$ e cujo elemento unidade é $\frac{1}{1}$, como vamos ver.
Comecemos por mostrar que a adição é comutativa; para isso basta ter em conta a definição da operação de adição e observar que o resultado $\frac{ad+bc}{bd}$ da adição $\frac{a}{b}+\frac{c}{d}$
não se altera se trocarmos a ordem das parcelas.
Para provarmos a associatividade, consideremos três elementos $\frac{a}{b},\frac{c}{d},\frac{e}{f}$ de Q.

Temos

$$(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+e(bd)}{(bd)f}=\frac{adf+bcf+ebd}{bdf}$$

e

$$\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})=\frac{a}{b}+\frac{cf+ed}{df}=\frac{a(df)+(cf+ed)b}{b(df)}=\frac{adf+cfb+edb}{bdf}$$

É imediato que os resultados encontrados são iguais.
Vejamos que $\frac{0}{1}$ é o zero. Para tal, basta mostrar que $\frac{0}{1}+\frac{a}{b}=\frac{a}{b}$. Ora

$$\frac{0}{1}+\frac{a}{b}=\frac{0b+a.1}{1b}=\frac{0+a}{b}=\frac{a}{b}$$

Que todos o elemento $\frac{a}{b}$ de Q admite simétrico do tipo $\frac{-a}{b}$ também é de fácil verificação. De facto, $\frac{a}{b}+\frac{-a}{b}=\frac{ab+(-a)b}{b^2}=\frac{ab+(-ab)}{b^2}=\frac{0}{b^2}$. Só falta ver que $\frac{0}{b^2}=\frac{0}{1}$.
Mas, por construção , resulta trivialmente que $0.1=0b^2$, para todo o b de D*.

Até agora provámos que (Q,+) é grupo comutativo. Mostremos de seguida que, em Q, a multiplicação goza das propriedades comutativa e associativa e admite elemento neutro.
Que a multiplicação é comutativa, resulta trivialmente da própria definição da operação de multiplicação. A associatividade obtem-se, observando que $(\frac{a}{b}\frac{c}{d})\frac{e}{f}=\frac{ac}{bd}\frac{e}{f}=\frac{(ac)e}{(bd)f}$

e que $\frac{a}{b}(\frac{c}{d}\frac{e}{f})=\frac{a}{b}\frac{ce}{df}=\frac{a(ce)}{b(df)}$. Por último, observemos que $\frac{1}{1}$ é o elemento neutro para a multiplicação. De facto é trivial que $\frac{a}{b}\frac{1}{1}=\frac{1}{1}\frac{a}{b}=\frac{a}{b}$. Para terminar a demonstração de que Q é corpo, falta verificar, por um lado, que todo o elemento não nulo de Q admite inverso multiplicativo e, por outro a propriedade distribuitiva em Q.

Quanto ao primeiro aspecto, notemos que dizer $\frac{a}{b}=0$ é equivalente a dizer $a=0$, uma vez que $0=\frac{0}{1}$ (Observe-se que $\frac{0}{b}=\frac{0}{1}\Leftrightarrow 0.1=0.b$).

Ou seja, se $\frac{a}{b}$ é um elemento não nulo de Q , então é do tipo $a\neq 0$ e $b\neq 0$. Mas sendo $a,b\neq 0$ então $\frac{b}{a}\in Q$. Ora, $\frac{a}{b}\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=1$.

Logo $\frac{a}{b}$ admite inverso da forma $\frac{b}{a}$.

Quanto à distribuitividade, basta mostrar que $(\frac{a}{b}+\frac{c}{d})\frac{e}{f}=\frac{a}{b}\frac{e}{f}+\frac{c}{d}\frac{e}{f}$ Mas

$$\left(\frac{a}{b}+\frac{c}{d}\right)\frac{e}{f}=\frac{ad+cb}{bd}\frac{e}{f}=\frac{(ad+cb)e}{(bd)f}=\frac{ade+cbe}{bdf}$$ e

$$\frac{a}{b}\frac{e}{f}+\frac{c}{d}\frac{e}{f}=\frac{ae}{bf}+\frac{ce}{df}=\frac{aedf+cebf}{bfdf}=\frac{(aed+ceb)f}{bdff}=$$

$$=\frac{aed+ceb}{bdf}\frac{f}{f}=\frac{aed+ceb}{bdf}$$

Resta-nos, para terminar a demonstração do teorema 3, provar como podemos considerar o domínio de integridade D isomorfo a um subdomínio do corpo Q. Para isso, consideremos $Q'=\{\frac{a}{1}, a\in D\}$ e vamos provar que $Q'\subset Q$ (Q' é subdomínio de Q) é isomorfo a D. Para verificar que Q' é um subdomínio de Q, temos de verificar que: i) Q' é subanel de Q; ii) Q' contem a identidade; iii) Q' não tem divisores de zero.

Ora $Q'\subset Q$ e $Q'\neq\varnothing$.

$\forall \frac{a}{1}, \frac{b}{1}\in Q', \frac{a}{1}-\frac{b}{1}\in Q'$

De facto, $\frac{a}{1}-\frac{b}{1}=\frac{a}{1}+\frac{-b}{1}=\frac{a-b}{1}\in Q'$

Por outro lado,

$\forall \frac{a}{1}, \frac{b}{1}\in Q', \frac{a}{1}\frac{b}{1}\in Q'$

De facto, $\frac{a}{1}\frac{b}{1}=\frac{ab}{1}\in Q'$

Logo Q' é subanel de Q e i) está verificada.

Que ii) se verifica, é imediato.

Para provar iii) suponhamos, por absurdo, que Q' admite divisores de zero. Seja $\frac{a}{1}$ um divisor de zero em Q'. Logo, $\exists \frac{a'}{1}\in Q'\backslash\{\frac{0}{1}\}: \frac{a}{1}\frac{a'}{1}=\frac{0}{1}$. Mas como $Q'\subset Q$, $\frac{a'}{1}\in Q$ e logo $\frac{a}{1}$ é divisor de zero em Q, o que é absurdo.

Logo Q' é um subdomínio de Q.
Vamos agora procurar o isomorfismo. Consideremos a aplicação $\varphi: D \to Q'$

$\ldots . a \to \dfrac{a}{1}$. É evidente que φ é sobrejectiva. Para provar a injectividade, consideremos dois elementos *a* e *a'* de D tais que $\varphi(a) = \varphi(a')$ ou seja, $\dfrac{a}{1} = \dfrac{a'}{1}$. Daqui resulta a=a' pelo que φ é injectiva. Falta provar que φ é homomorfismo de aneis. Ora, $\varphi(a+b) = \dfrac{a+b}{1} = \dfrac{a}{1} + \dfrac{b}{1} = \varphi(a) + \varphi(b)$.

Analogamente $\varphi(ab) = \dfrac{ab}{1} = \dfrac{a}{1}\dfrac{b}{1} = \varphi(a)\varphi(b)$. Logo φ é um isomorfismo. De tudo o que foi dito, concluímos que Q é um corpo que contém um subdomínio isomorfo a D, c.q.d. ♣

Já foi dito que o corpo Q que construimos é chamado corpo dos quocientes de D. A partir de agora podemos esquecer o modo como tal corpo foi encontrado e pensamos apenas nas suas propriedades: todo o elemento de Q pode ser escrito sob a forma de um quociente de dois elementos de D. Em particular, usaremos a notação ab^{-1} para representar $\dfrac{a}{b}$.

Contudo, preste-se atenção para que não se caia no erro grosseiro de considerar que para duas fracções $\dfrac{a}{b}$ e $\dfrac{c}{d}$ serem iguais é necessário que $a=c$ e $b=d$. Note-se que a fracção $\dfrac{a}{b}$ não é um par de elementos de D, onde $b \neq 0$, mas é representante de uma classe de pares de elementos de D.
Em particular, se fizermos D=Z (mostra-se que Z é domínio de integridade) e atendendo às considerações feitas, encontramos o corpo Q dos números racionais.

SUBCORPOS E EXTENSÕES

Definição 15
Seja (K,+,.) um corpo e S um subconjunto de K. Diremos que S é um subcorpo de K se S é um subanel de K que é um corpo sobre as operações (+) e (.). Diremos dualmente que K é uma extensão de S se S é subcorpo de K.

Definição 16
Seja K uma extensão do corpo S e M um subconjunto de K. Chamamos extensão de S por adjunção de M e representamos por S(M) à intersecção de todos os subcorpos de K que contém $S \cup M$.
Das próprias definições é óbvio que:
- $S \subset S(M) \subset K$
- $S(M) = S$ se e só se $M \subset S$

SUBGRUPO NORMAL. GRUPO QUOCIENTE

Definição 17
Seja G um grupo e H um subgrupo de G. Diz-se que H é subgrupo normal de G e escreve-se $H \triangleleft G$ se $xH=Hx$, para todo o $x \in G$.

Proposição 4
Se G é um grupo abeliano então qualquer seu subgrupo é subgrupo normal.

Demonstração:
Seja H um subgrupo de G. Vamos provar que $xH=Hx$, para todo o $x \in G$. Seja $x \in G$, arbitrário. Então
$xH = \{xh: h \in H\} = \{hx: h \in H\} = Hx$ c.q.d. ♣

Vamos de seguida ver, como, de um grupo e de um subgrupo normal, podemos obter um novo grupo.
Seja então G um grupo e H um seu subgrupo e consideremos a relação de equivalência R definida por $aRb \Leftrightarrow b^{-1}a \in H$, com $a,b \in G$. Que a relação R é reflexiva, resulta do facto de que, para todo o $a \in G$, $aa^{-1} = e \in H$. (Porque H é subgrupo de G, o elemento unidade tem de pertencer a H). Para provar a simetria de R, considerem-se a,b$\in$G tais que aRb. Então $b^{-1}a \in H$ e, sendo H um subgrupo, se contém um elemento também contém o seu inverso. Portanto $(b^{-1}a)^{-1} \in H$, ou seja, $a^{-1}b \in H$ o que significa que *bRa.*
Para a transitividade, consideremos $a,b,c \in G$ tais que *aR*b e *bRc.* Vamos provar que então *aRc.* Por hipótese $b^{-1}a \in H$ e $c^{-1}b \in H$ e, como H é subgrupo resulta $(c^{-1}b)(b^{-1}a) \in H$. Ou seja, $c^{-1}a \in H$ o que significa *cRa.* Como à relação R é reflexiva, simétrica e transitiva é uma relação de equivalência. Vamos definir , sendo $a \in G$, a classe de equivalência $[a]_R$ tal que

$$[a]_R = \{x \in G : xRa\} = \{x \in G : a^{-1}x \in H\} = \{x \in G : a^{-1}x = h, h \in H\} =$$
$$= \{x \in G : x = ah, h \in H\} =$$
$$= \{ah, h \in H\} = aH$$

Designemos por $G' = \{aH, a \in G\}$. Vimos então que G' é a partição de G correspondente à relação de equivalência atrás definida. Forme-se o conjunto quociente $G/R = \{[a]_R : a \in G\}$, ou seja $G'=G/R$. Representemos este conjunto por G/H ; isto é, $G/H = \{ah\colon h \in H\}$, com $G/H \neq \emptyset$ já que $eH = H \in G/H$ .Em G/H vamos definir um produto tal que $(aH)(bH) = (ab)H$, para todos os aH e bH de G/H. Pretende-se que tal produto seja uma aplicação de G/HxG/H em G/H; ou seja, pretende-se que

i) $\forall aH, bH \in G/H, (aH)(bH) \in G/H$

ii)
$\forall aH, a'H, bH, b'H \in G/H, aH = a'H \wedge bH = b'H \Rightarrow (ab)H = (a'b')H$

Como $a,b \in G$, tem-se que $ab \in G$ e logo $(ab)H \in G/H$. Falta garantir que, se $a' \in aH$ e $b' \in bH$ então $a'b' \in (aH)(bH) = (ab)H$. Vejamos que esta compatibilidade resulta do facto de H ser subgrupo normal de G. Seja $a' \in aH$. Então $a'=ah_1$ com $h_1 \in H$. Por outro lado, sendo $b' \in bH$, $b'=bh_2$, para algum $h_2 \in H$. Logo $a'b' = (ah_1)(ah_2) = a(h_1 b)h_2$. Como H é subgrupo normal de G, $Hb=bH$ e portanto, dado $h_1 \in H$, existe $h'_1 \in H$. tal que $h_1 b=bh'_1$. De onde $a'b' = a(bh'_1)h_2 = ab(h'_1 h_2) = (ab)h$ com $h = h'_1 h'_2 \in H$, porque H é subgrupo. Logo, $a'b \in (ab)H$, como pretendíamos.

Vejamos agora que a operação interna $\begin{array}{l} G/H x G/H :\rightarrow G/H \\ ..(aH,bH)...\rightarrow (ab)H \end{array}$ confere a G/H a estrutura de grupo.

Sejam $aH, bH, cH \in G/H$. Então
$$\begin{aligned}&[(aH)(bH)](cH) = ((ab)H)(cH) = ((ab)c)H = (a(bc))H = \\ &= (aH)((bc)H) = (aH)[(bH)(cH)]\end{aligned}$$
o que significa que a operação é associativa. Por outro lado, para qualquer $a \in G$, $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$ o que significa que eH é elemento neutro em G/H. Quanto à existência de elemento inverso e sendo $a \in G$, temos que $(aH)(a^{-1}H) = (aa^{-1})H = eH = (a^{-1}a)H = (a^{-1}H)(aH)$. Ou seja, o inverso do elemento aH é $a^{-1}H$. Note-se que, sendo $a \in G$ e G um grupo, existe $a^{-1} \in G$ e portanto $a^{-1}H$ existe e pertence a G/H. De tudo o que vimos, podemos concluir que G/H é grupo para a operação atrás definida. Este grupo designa-se por grupo quociente de G por H.

IDEAL DE UM ANEL
ANEL QUOCIENTE

Definição 18

Um subconjunto não vazio R de um anel A diz-se um <u>ideal</u> se:

(i) R é subanel de A

(ii) Para todos os $r \in R$ e $a \in A$, $ar \in R$ e $ra \in R$

Vimos que a noção de subgrupo normal, permite construir, a partir de um grupo e de um subgrupo, um novo conjunto que designamos por grupo quociente. Ora, a definição de ideal é, na teoria doas anéis, a que corresponde à noção de subgrupo normal na teoria dos grupos. Vemos como a noção de ideal permite construir a partir de um anel e de um subanel, um novo anel que desiganremos por anel quociente.

Seja R um anel e S um subanel de R. Como (S,+) é subgrupo de (R,+) e (R,+) é abeliano, pela proposição 2, (S,+) é subgrupo normal de (R,+) pelo que podemos pensar no grupo quociente R/S. Pretende-se definir em R/S uma estrutura multiplicativa de tal modo que R/S seja um anel. Defina-se uma multiplicação tal que

$R/SxR/S:\rightarrow R/S$

$(r+S, r'+S) \rightarrow (r+S)(r'+S) = rr'+S$

que seja compatível com a estrutura das classes; isto é, pretende-se que os elementos da forma $(r+s_1),(r'+s_2)$ pertençam à classe produto, para quaisquer $r, r' \in R$ e $s_1, s_2 \in S$. Analisemos os diversos casos possíveis. Sejam s_1,s_2 elementos de S.

Se r=0 e r'=0 então

$(r+S)(r'+S) = (0+s_1)(0+s_2) = 0+S = S$.

Se r=0 e r'≠0 então

$(0+s_1)(r'+s_2) = 0r'+0s_2 + s_1r'+s_1s \in 0+S$

$\Rightarrow \exists s \in S: s_1r'+s_1s_2 = s \Rightarrow \exists s \in S = s_1r' = s - s_1s_2 \Rightarrow s_1r' \in S$.

Se r≠0 e r'=0, então
$(r+s_1)(0+s_2)=r0+rs_2+s_1 0+s_1 s_2 \in 0+S$
$\Rightarrow \exists s \in S: rs_2+s_1 s_2=s, \Rightarrow \exists s \in S: rs_2=s-s_1 s_2 \Rightarrow rs_2 \in S$.

Se r≠0 e r'≠0 então $(r+s_1)(r'+s_2)=rr'+S$
$\Rightarrow \exists s \in S: rr'+rs_2+s_1 r'+s_1 s_2=rr'+s \Rightarrow \exists s \in S: rs_2+s_1 r'+s_1 s_2=s$
$\Rightarrow \exists s \in S: rs_2+s_1 r'=s-s_1 s_2 \Rightarrow rs_2+s_1 r' \in S$

Concluímos assim que, para definir em R/S uma estrutura multiplicativa compatível com a estrutura das classes, temos de exigir que:

- S seja subanel
- Para todo os $r \in R$ e $s \in S$ se tenha $rs \in S$ e $sr \in S$.

Resumindo, para definir em R/S uma estrutura multiplicativa compatível com a estrutura das classes temos que exigir que S seja ideal de R.
Conclusão: se I é um ideal de R, podemos definir em R/I uma adição e uma multiplicação compatíveis com a esturutra das classes e que conferem a R/I a estrutura de anel. O anel assim obtido designa-se por anel quociente.
Vamos agora ver que o anel quociente satisfaz uma propriedade fundamental.

Definição 19
Seja $\varphi: R \to R'$ um homomorfismo de anéis. Chama-se <u>núcleo</u> de φ e representa-se por Ker(φ) à pré-imagem de $\{0_{R'}\}$; isto é, $Ker(\varphi)=\{x \in R: \varphi(x)=0_{R'}\}$.

Teorema 4
Sendo I um ideal de anel R, existe um homomorfismo de anéis de domínio R cujo núcleo é exactamente I.

Demonstração:

Como I é um ideal de R, podemos considerar o anel quociente R/I. Consideremos a aplicação $\begin{array}{l} p: R \rightarrow R/\mathrm{I} \\ \ldots\ldots r \rightarrow r+\mathrm{I} \end{array}$ e vamos provar que é um homomorfismo de anéis, cujo núcleo é exactamente I. Sejam $r, r' \in R$ arbitrários. Ora $p(rr') = rr'+\mathrm{I} = (r+\mathrm{I})(r'+\mathrm{I}) = p(r)p(r')$. Considerando agora a operação de adição tem-se, para $r, r' \in R$ arbitrários, $p(r+r') = (r+r')+\mathrm{I} = (r+\mathrm{I})+(r'+\mathrm{I}) = p(r)+p(r')$. Provamos então que p é um homomorfismo. Por outro lado

$Ker(p) = \{r \in R: p(r) = 0+\mathrm{I}\} = \{r \in R: r+\mathrm{I} = 0+\mathrm{I}\} = \{r \in R: r \in \mathrm{I}\} = \mathrm{I}$,como se pretendia. ♣

Como consequência, verifica-se ainda uma propriedade de $R / Ker(\varphi)$. Antes porém apresentemos uma definição.

Definição 20

Chama-se epimorfismo a todo o homomorfismo sobrejectivo.

Proposição 5

Seja $\varphi: R \rightarrow R'$ um epimorfismo de anéis. Então $R / Ker(\varphi)$ e R' são isomorfos ; isto é $R / Ker(\varphi) \cong R'$.

Demonstração: (sem demonstração)

Proposição 6

Seja $\varphi: R \rightarrow R'$ um homomorfismo de anéis. φ é injectiva se e só se Ker(φ)={0}.

Demonstração:

(⇒)

Se φ é injectiva e φ(r)=0 então φ(r)= φ(0) e daí r=0 (trivial).

($\Leftarrow$)
Se Ker(φ)={0}, consideremos $r, r' \in R$ tais que φ(r)=φ(r'). Logo $0 = \varphi(r) - \varphi(r') = \varphi(r - r')$ porque φ é homomorfismo. De onde $0 = r - r' \Leftrightarrow r = r'$ e portanto φ é injectiva. ♣

IDEAL PRIMO. IDEAL MAXIMAL.

Definição 21
Seja R um anel e X um subconjunto de R. Chama-se <u>ideal gerado por</u> X à intersecção de todos os ideais de R que contêm X.

Proposição 6
Seja R um anel comutativo com identidade e X um subconjunto não vazio de R. Então o ideal de R gerado por X é

$$RX = \{\sum_{i=1}^{n} r_i x_i \, , r_i \in R, x_i \in X, i = 1, \ldots, n, n \geq 1\} \, .$$

Demonstração: (sem demonstração)

Definição 22
Um <u>ideal</u> P diz-se <u>primo</u> se, sempre que $xy \in P$ então $x \in P$ ou $y \in P$

O resultado seguinte é uma caracterização dos ideais primos de um anel comutativo com elemento unidade.

Teorema 5
Seja $R \neq \{0\}$ um anel comutativo com elemento unidade. Seja N um ideal próprio de R. Então N é um ideal primo se e só se R/N é um domínio de integridade.

Demostração

($\Rightarrow$)

Seja N um ideal primo de R . Sabemos que R/N é um anel, comutativo com elemento unidade. Para provar que R/N é domínio de integridade, basta provar que em R/N não existem divisores de zero. Seja $a+N$ um elemento não nulo de R/N, (isto é $a+N \neq N$). Vamos ver que a igualdade $(a+N)(b+N)=N$ só é possível com $b+N=N$. De facto, $(a+N)(b+N)=N \Leftrightarrow ab+N=N \Leftrightarrow ab \in N \Rightarrow a \in N \vee b \in N$, uma vez que N é ideal primo. Ora, por hipótese, $a \notin N$; então $b \in N$ e logo $b+N=N$, como pretendíamos.

($\Leftarrow$)

Seja R/N um domínio de integridade e N um ideal próprio de R. Queremos provar que N é um ideal primo. Seja $ab \in N$. Então $ab+N=N$; ou seja, $(a+N)(b+N)=N$. Mas, como R/N não tem divisores de zero tem-se que $a+N=N$ ou $b+N=N$. Isto é, $a \in N$ ou $b \in N$, o que prova que N é ideal primo, como se pretendia. ♣

Definição 23

Um ideal M de um ideal R diz-se um ideal maximal se $M \neq R$ e se não existe nenhum ideal próprio de R que contenha M, propriamente.

Teorema 6

Seja R um anel comutativo com elemento unidade e M um ideal de R. M é um ideal maximal se e só se R/M é um corpo.

Demonstração:

($\Rightarrow$)

Seja M um ideal maximal de R. Então $M \neq R$ e portanto R/M tem pelo menos um elemento não nulo. Como R é um anel comutativo com elemento unidade, também R/M é anel comutativo com elemento unidade. Para provar que R/M é corpo, temos de garantir que todo o elemento não nulo de R/M admite inverso multiplicativo. Seja

$a+M \neq M$ um elemento não nulo de R/M. Pretendemos provar que existe $b+M \in R/M$ tal que $(a+M)(b+M)=1+M$.
Seja $X=\{a\} \cup M$; consideremos o ideal gerado por X e que representamos por (X). Como M é um ideal maximal de R, deverá ter-se (X)=R . De facto, se $(X) \subset R$ e uma vez que $M \subset (X)$ já que $a \notin$ M por hipótese, e $a \in (X)$ M não seria um ideal maximal de R, contrariando a hipótese. Então (X)=R e logo $1 \in (X)$. Pela proposição 5, $(X)=\{ar+m, r \in R, m \in M\}$ e portanto tem-se $1=ar+m$, para algum r de R e algum m de M. Então $ar=1-m$; logo $ar \in 1+M$. Donde resulta que $ar+M=1+M$ e logo $(a+M)(r+M)=1+M$, pelo que está garantida a existência de um elemento $b+M \in R/M$ tal que $(a+M)(b+M)=1+M$, como pretendíamos.

($\Leftarrow$)
Suponha-se que R/M é um corpo. Então R/M tem pelo menos um elemento não nulo e portanto M≠R . Para provar que M é ideal maximal, temos de provar que não existe nenhum ideal próprio de R que contenha M propriamente. Por absurdo, suponhamos que existe um ideal M'≠R tal que M⊂M' . Mas, como M'⊂R, existe $a \in R$ tal que $a \notin M'$ e, como M⊂M' existe $b \in M'$ tal que $b \notin M$. Vejamos que tal situaçaõ vai conduzir ao absurdo. Como, por hipótese R/M é corpo e $b+M \neq M$, tem-se que, existe $b'+M \in R/M$, tal que $(b+M)(b'+M)=1+M$
Daqui resulta $(b+M)(b'+M)(a+M)=a+M$. Ou seja, existe $c+M \in R/M$ tal que $(b+M)(c+M)=a+M$. De onde $bc+M=a+M$ e logo $(bc-a) \in M$
Atendendo a que M⊂M' tem-se que $(bc-a) \in M'$ e logo $bc+M'=a+M'$
Ou seja $(b+M')(c+M')=a+M'$ e como $b \in M'$ resulta $b+M'=M'$, isto é, $b+M'$ é o zero de R/M' .Mas como o zero de um anel, multiplicado por qualquer outro elemento é sempre igual a zero do anel, vem que $a+M'=M'$ e logo $a \in M'$, o que contraria a escolha de a. O absurdo resultou de se ter suposto que existia um ideal próprio M' contendo propriamente M, o que supunha que M não era maximal. Então M é ideal maximal, como pretendiamos. ♣

Definição 24

Seja A um anel comutativo com elemento identidade 1. Um elemento a de A diz-se uma unidade se $c.a=1=a.c$, para algum $c \in A$.
U(A) representa o conjunto de todas as unidades de A.

Definição 25

Seja D um domínio de integridade e $r,s \in D$. Diz-se que r divide s (simbolicamente $r \backslash s$) se existe $k \in D$ tal que $s=kr$.

Definição 26

Seja D um domínio de integridade e $r \in D$. Um elemento r diz-se elemento primo em D sse:

i) $r \neq 0$ e $r \in U(D)$

i) dados $a,b0 \in D$ sempre que $r \backslash ab$ então $r \backslash a$ ou $r \backslash b$.

Teorema 7

Seja D um domínio de integridade e $p \in D \backslash \{0\}$. Então p é primo em D se e só se $(p) = \{rp, r \in D\}$ é um ideal próprio primo.

Demonstração:

Designemos por $D^* = D \backslash \{0\}$.

$(\Rightarrow)$

Seja $p \in D^*$ tal que p é primo. Então $p \notin U(D)$ e $p \neq 0$ pelo que (p) é ideal próprio de D.

Seja $xy \in (p)$. Então $xy=rp$ para algum $r \in D$ o que significa que $p \backslash (xy)$. Como p é primo tem-se $p \backslash x$ ou $p \backslash y$. Se $p \backslash x$ então $x=k_1p$, com $k_1 \in D$ pelo que $x \in (p)$. Se $p \backslash y$ e analogamente, se conclui que $y \in (p)$. Mas assim concluimos que, se $xy \in (p)$ então $x \in (p)$ ou $y \in (p)$, o que significa que (p) é um ideal primo.

$(\Leftarrow)$

Suponha-se que (p) é um ideal próprio primo de D. Como $p \in D^*$, $(p) \neq \{0\}$. Pelo teorema 4 D/(p) é um domínio de integridade. Então

$1+(p)\neq(p)$ e portanto $1\notin(p)$. Então, para todo $r\in D$, $rp\neq 1$ o que significa que $p\notin U(D)$. Por outro lado, sejam $a,b\in D$ tais que $p\backslash(ab)$. Isto é, $ab=kp$, para algum $k\in D$, o que significa que $ab\in(p)$. Consequentemente $a\in(p)$ ou $b\in(p)$, porque, por hipótese (p) é ideal primo. Mas então resulta que $p\backslash a$ ou $p\backslash b$. Concluímos assim que p é um elemento de D tal que

$$\begin{array}{l} p\neq 0, p\notin U(D) \\ p\backslash(ab)\Rightarrow p\backslash a \vee p\backslash b \end{array}$$ o que significa que p é um elemento primo de D, como se pretendia. ♣

Extensões Simples
Extensões Algébricas e Transcendentais

Definição 27

Seja K um corpo, S um subcorpo de K e $\theta \in K$. Chama-se <u>extensão simples</u> de S à extensão de S por adjunção de θ e representa-se por $S(\theta)$.

Teorema 8

Seja K um corpo, S um subcorpo de K e $\theta \in K$. Então $S(\theta)$ é o menor subcorpo de K que contém $S \cup \{\theta\}$.

Demonstração:

Consideremos o conjunto $\overline{K}$ tal que

$$\overline{K} = \{\frac{a_0 + a_1\theta + ... a_n\theta^n}{b_0 + b_1\theta + ... + b_m\theta^m}, a_i, b_j \in S, i = 0,..., n, j = 0,..., m, n, m \in N_0,$$
$$b_0 + b_1\theta + ... + b_m\theta^m \neq 0\}$$

onde, por definição

$$\frac{a_0 + a_1\theta + ... a_n\theta^n}{b_0 + b_1\theta + ... + b_m\theta^m} = (a_0 + a_1\theta + ... + a_n\theta^n)(b_0 + b_1\theta + ... + b_m\theta^m)^{-1}.$$

Vamos provar que $\overline{K}$ é o menor subcorpo de K que contém $S \cup \{\theta\}$. Seja K_1 um subcorpo de K que contém $S \cup \{\theta\}$. Como K_1 contém θ e, em particular, K_1 é ainda um corpo, contém todas as potências multiplicativas de θ e portanto $\theta^i \in K_1$, i=0,1, ... Mas então também são elementos de K_1 todos os polinómios $a_0 + a_1\theta + ... + a_n\theta^n$ com $a_j \in S, j = 0, \dots, n$ e também os seus inversos. Logo, para todos os $a_j \in S, j = 0, \dots, n$ e para todos os $b_k \in K_1, k = 0, \dots, m$ tem-se $(a_0 + a_1\theta + ... + a_n\theta^n)(b_0 + b_1\theta + ... + b_m\theta^m)^{-1} \in K_1$ desde que $b_0 + b_1\theta + ... + b_m\theta^m \neq 0$. Mas então $\overline{K} \subset K_1$ e portanto $\overline{K}$ é o menor subcorpo que contem $S \cup \{\theta\}$. Donde, por definição, resulta $\overline{K} = S \cup \{\theta\}$; isto é, $\overline{K} = S(\theta)$ ♣

Recordando que podemos designar por $S[\theta]$ o anel dos polinómios sobre S na indeterminada θ, verifica-se que $S[\theta] \subset S(\theta)$.

Definição 28
Seja K um corpo, S um subcorpo de K e $\theta \in K$. Se $S(\theta) \equiv S[\theta]$ diz-se que <u>θ é algébrico sobre S</u> e que S(θ) é a <u>extensão algébrica</u> de S por adjunção de θ .

Definição 29
Seja K um corpo, S um subcorpo de K e $\theta \in K$. Diz-se que <u>θ é transcendente</u> sobre S se $S(\theta) \supset S[\theta]$ e que S(θ) é a <u>extensão transcendente</u> de S por adjunção de θ .

Para distinguirmos extensões algébricas de extensões transcendentes, consideremos o teorema seguinte.

Teorema 9
Seja K um corpo, S um subcorpo de K e $\theta \in K$. Então verifica-se uma e uma só das seguintes condições:
i) $S(\theta) \approx S(X)$
ii) $S(\theta) \approx S[X]/\varphi$
onde $\varphi \in S[X]$ é um polinómio irredutível na indeterminada x e S(X) representa o corpo das fracções de $S[X]$
Antes porém da demonstração deste teorema, recordemos a definição de polinómio irredutível.

Definição 30
Seja K um corpo e $p \in K[X]$ Diz-se que p é um <u>polinómio irredutível</u> <u>se:</u>

I) p não é um polinómio constante;
ii) para todos os $g,h \in K[X]$, se p=gh, então ou h é um polinómio constante não nulo ou g é um polinómio constante não nulo.

Passemos, agora sim, à demostração do teorema 8.

Demonstração:

Consideremos a aplicação
$$\begin{array}{c} \varphi: S[X] \to S(\theta) \\ \sum_{j=0}^{n} a_j x^j \to \sum_{j=0}^{n} a_j \theta^j \end{array}$$

Facilmente se verifica que φ é um epimorfismo de anéis, se S(θ) é uma extensão algébrica de S. Então, pela Proposição 3 $S[X] / Ker\varphi \cong S[\theta]$. Temos então dois casos a considerar:

(i) $Ker\varphi = \{0\}$

Pela Proposição 4, φ é injectiva e logo S[X]≅S[θ]. Como K é um corpo, S[X] é domínio de integridade e logo S[θ] também é domínio de integridade. Logo, são também isomorfos os corpos das fracções de S[X] e S[θ]. Temos então S(X)≅S(θ), o que prova (i).

(ii) $\{0\} \neq Ker\varphi \subset S[X]$

Como S é um corpo, S[X] resulta um domínio de ideais principais. Então, existe ψ∈S[X] tal que $Ker\varphi = (\psi)$ e então S[θ]≅S[X]/(ψ) . Como S é corpo, S[θ] é domínio de integridade e tem-se que S[X]/(ψ) é um domínio de integridade. Pelo Teorema 4 concluímos que (ψ) é um ideal primo. Mas então o Teorema 6 garante que ψ é um polinómio primo. Como S[X] é um domínio de integridade tem-se que ψ é um polinómio irredutível. Por outro lado, sendo (ψ) um ideal maximal, o Teorema 5 garante que S[X]/(ψ) é um corpo. Mas então S[θ] é corpo e, por definição de extensão , S(θ)=S[θ]. Então S(θ)≅S[θ]/(ψ) com ψ∈S[X], irredutível, o que completa a demonstração. ♣

BIBLIOGRAFIA

Godement, R. (1966) *Cours d'Algébre.* Paris. Hermann

Santos, V. , Apontamentos de Álgebra, Universidade de Aveiro.

(1994).Apontamentos de Álgebra, Mestrado da Universidade de Coimbra