ÁLGEBRA
Um Guia de Estudo

4ª Edição

Marco Aurélio Palumbo Cabral
mcabral@labma.ufrj.br

Laboratório de Matemática Aplicada - Dep. 05
Instituto de Matemática - U.F.R.J.
Caixa Postal 68530 - CEP 21945 - Rio de Janeiro - RJ

SUMÁRIO:

I – Prefácio

Gostaria de dedicar esta monografia ao Prof. Felipe Acker, meu orientador de iniciação científica, que foi o principal motivo de meu entusiasmo pela Matemática. Embora tenha feito este trabalho sem sua orientação — assumindo pessoalmente o risco de qualquer tropeço — sua influência se faz presente no modo como o material está apresentado.

Além disto gostaria de agradecer aos meus colegas Victor Giraldo e Maria Darci Godinho, sem os quais me teria faltado motivação para encerrar o presente. Agradeço também a turma da qual fui monitor pelas dúvidas e sugestões. Gostaria de agradecer a Fátima Lins pela leitura atenta e correção de diversos erros da 3ª edição. Para esta 4ª edição foi modificado o layout, incluímos novos exercícios e melhoramos a redação de forma geral.

Gostaria, por fim, de agradecer o Laboratório de Matemática Aplicada, o Instituto de Matemática e ao CNPq, pelo suporte financeiro.

Rio de Janeiro, Maio/1991

II – Introdução

Esta monografia foi feita com base na minha experiência como monitor da disciplina ÁLGEBRA II oferecida aos alunos do ciclo básico de Matemática do IM – UFRJ.

Logo percebi a grande dificuldade dos alunos compreenderem os conceitos principais: Classes de Equivalência, Anel Quociente, Teorema do Homomorfismo, Automorfismos de Corpos, etc.

Se em determinados momentos posso não ser inteiramente formal, deixando este trabalho para livros de consulta, procuro dar aqui a maneira como os conceitos são pensados e utilizados em linguagem coloquial. Procuro fazer analogias com Álgebra Linear, que tem forte apelo intuitivo.

Como referências principais o livro Introdução à Álgebra de Adilson Gonçalves — que contém muitos exercícios, alguns dos quais retirei explicitamente com a devida menção ao longo do texto — e Álgebra: Um curso de Introdução, de Arnaldo Garcia e Ives Lequain. Outro livro excelente é A First Course in Abstract Algebra (John B. Fraleigh).

III – Função

1) Introdução

Admitiremos conhecida a teoria elementar de conjuntos, ou seja, as definições de pertinência, contido, etc. e a noção intuitiva de função: Uma $f : A \longrightarrow B$ é "uma coisa" que associa a todo elemento do conjunto A, o domínio da função, um único elemento do conjunto B, o contradomínio.

2) Definições

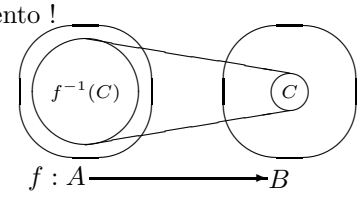
Definição: DOMÍNIO – Conjunto onde f está definida, ou seja, o conjunto A acima.

Definição: CONTRADOMÍNIO – Conjunto onde f assume valores (conjunto B acima).

Definição: IMAGEM – Subconjunto do contradomínio onde seus elementos tem ao menos um correspondente no Domínio. Denota-se e define-se $\mathrm{Im}(f) = \{b \in B; b = f(a) \text{ com } a \in A\}$.

Definição: IMAGEM INVERSA – Denota-se e define-se: $f^{-1}(C) = \{a \in A; f(a) \in C\}$. A imagem inversa é um subconjunto do domínio.

Obs: Não confundir com função inversa, que associa elementos de B a A. A imagem inversa é um conjunto, e não um elemento !



Definiremos agora dois conceitos fundamentais: Função Sobrejetiva, que assegura que o contradomínio e a imagem são o mesmo conjunto; e Função Injetiva, que assegura que a cada elemento da imagem corresponde somente um elemento do domínio. Juntando estas duas características definimos

a Função Bijetiva, que implica na existência de uma função inversa f^{-1}.

Definição: FUNÇÃO INJETIVA – Se $f(a) = f(b)$ implica que $a = b$.

Definição: FUNÇÃO SOBREJETIVA – Se $\forall b \in B, \exists a \in A; f(a) = b$.

Definição: FUNÇÃO BIJETIVA – Quando é sobrejetiva e injetiva ao mesmo tempo.

Definição: FUNÇÃO INVERSA – Quando uma função é bijetiva podemos definir uma função inversa f^{-1}, que associa para todo $b \in B$, um $a \in A; f^{-1}(b) = a$.

Definição: FUNÇÃO IDENTIDADE – Uma função $f : A \longrightarrow A; f(a) = a$.

Conforme já foi visto, nos deparamos com dois problemas quando queremos inverter uma função (torná-la uma bijeção). O primeiro é o fato da função não ser sobrejetiva, que pode facilmente ser contornado, bastando redefini-la para que o contradomínio seja Im(f), ou $f : A \longrightarrow$ Im(f). (Pense nisto !!!) Para evitar a não injetividade teremos que aprender antes o importante conceito de classe de equivalência, o que faremos logo adiante.

Para definirmos conjunto finito precisamos da seguinte notação: I_n o subconjunto dos números entre 1 e n.

Definição: CONJUNTO FINITO – Todo conjunto que podemos estabelecer uma bijeção com I_n, onde "n" será chamado a cardinalidade do conjunto, ou seu número de elementos.

Definição: CONJUNTO INFINITO – Quando não é finito.

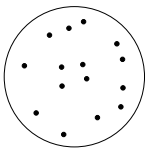
Definição: CONJUNTO INFINITO ENUMERÁVEL – Aquele que podemos estabelecer uma bijeção com $\mathbb{N}$.

Exercício: Tente estabelecer uma bijeção de $\mathbb{N}$ em $\mathbb{Z}$, $\mathbb{N}$ em $\mathbb{Q}$ e $\mathbb{N}$ em $\mathbb{R}$, e daí conclua quem é infinito enumerável, quem não é.

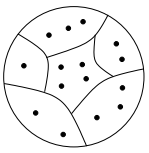
IV – Relação de Equivalência

Antes de vermos a definição formal gostaria de passar a idéia intuitiva que está por trás deste conceito. A metáfora que utilizaremos será a de uma prato, representando um conjunto, onde seus elementos são os átomos que o constituem. Joguemos este prato no chão para quebrá-lo ! Ele se partirá e teremos cacos de diversos tamanhos no chão.

Pensemos agora neste novo conjunto, onde cada elemento é um caco (ao invés de um átomo). Denotaremos por C este conjunto dos cacos do prato, e por P o conjunto de átomos do prato. A idéia importante é ver que o conjunto P foi partido, formando um novo conjunto C, onde os elementos são cacos.



P



C

Agora temos que para quaisquer átomos a, b e c pertencentes ao prato P:

(i) Cada átomo pertence a um caco.

(ii) Se a pertence a um mesmo caco que b então b pertence ao mesmo caco que a.

(iii) Se a pertence ao mesmo caco que b, b pertence ao mesmo caco que c, então a pertence ao mesmo caco que c.

Agora começaremos a definir os termos técnicos associados a estas idéias intuitivas. Uma relação é uma propriedade que dois elementos de um conjunto podem ter entre si. No caso em estudo a propriedade é pertencer ao mesmo caco. Denotaremos $a \sim b$ para dizer que o átomo a pertence ao mesmo caco que o átomo b.

Obs: Pode-se definir formalmente relação com pares ordenados: Uma relação num conjunto A será um subconjunto de $A \times A$ (lê-se A cartesiano A). Esta definição informal, neste caso, nos basta.

Definição: RELAÇÃO de EQUIVALÊNCIA – Uma relação "$\sim$" num conjunto A será de equivalência quando respeitar as seguintes propriedades $\forall\, a, b, c \in A$,

(i) $a \sim a$ (Reflexiva)

(ii) $a \sim b$ implica que $b \sim a$ (Simétrica)

(iii) $a \sim b$ e $b \sim c$ implica que $a \sim c$ (Transitiva)

Exercícios: Leia novamente os ítens (i), (ii) e (iii) relativos a átomo e caco dados acima e compare com a definição de relação de equivalência.

Exemplo: A relação em $\mathbb{R}^2$, x e y retas , $x \sim y$ se, e somente se $x \parallel y$ (x e y são retas paralelas) é relação de equivalência (verifique !).

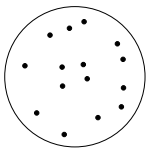
Vamos denotar para cada átomo $a \in P$, o caco a que o átomo pertence por $\bar{a} \in C$. Este caco será chamado classe de equivalência de a. Vemos portanto que cada classe de equivalência do conjunto P (o prato) será um caco.

Definição: CLASSE de EQUIVALÊNCIA – Seja $a \in A, \bar{a} = \{b \in A; a \sim b\}$ será a classe de equivalência de $a \in A$.

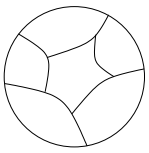
Definição: CONJUNTO QUOCIENTE – É o conjunto das classes de equivalência de um conjunto, denotando-se $A/\sim = \{\bar{x}; x \in A\}$ (Lê-se A dividido pela relação de equivalência).

Obs1: Na nossa analogia, o conjunto quociente de P (o prato) é o conjunto C, onde cada elemento é um caco, ou seja, $P/\sim = C$.

Obs2: O conjunto A e $A/\sim$ não está contido um no outro, nem vice-versa. Isto tem que ficar bem claro: Os elementos são distintos, como se dado um conjunto de bananas e outros de laranjas fosse perguntado quem está contido em quem ! Observe a figura abaixo.



A



$A/\sim$

Obs3: Poderia definir o que é uma partição de um conjunto e mostrar que toda relação de equivalência determina uma partição e vice-versa. Uma partição seria separar um conjunto em subconjuntos com intersecção vazia e com união dando o conjunto todo.

Exemplo: Frações e $\mathbb{Q}$. Seja $F = \{a/b; a, b \in \mathbb{Z}, b \neq 0\}$ o conjunto das frações. Exemplos de elementos de F são: $2/3, 7/4, 10/5, 3/2 \ldots$

Começaremos notando que $10/5$ e $2/1$ são elementos distintos de F representando o mesmo elemento de $\mathbb{Q}, 10/5 = 2/1 = 2 \in \mathbb{Q}$. Dado um elemento de F podemos corresponder um único elemento de $\mathbb{Q}$ de maneira óbvia, no entanto um elemento de $\mathbb{Q}$ possui infinitas representações em F. Exemplo: $0.5 = 1/2 = 2/4 = 3/6 = \ldots$

Queremos que estes elementos de F sejam considerados equivalentes. De fato definimos a seguinte relação de equivalência em F (verifique !): $a/b \sim c/d$ se, e somente se $ad = bc$ (em $\mathbb{Z}$). Desta forma podemos fazer $F/\sim$ isomorfo a $\mathbb{Q}$ (ver apêndice 5). Exemplos de elementos de $F/\sim$: $\{7/3, 14/6, 21/9, \ldots\}, \{2/3, 4/6, 6/9, \ldots\}$

Resumindo: Dado um conjunto A e uma relação de equivalência "$\sim$", esta quebra o conjunto A determinando um novo conjunto $A/\sim$, cujos elementos são classes de equivalência.

Exercícios:

1) Mostre que é relação de equivalência:
   a) $x, y \in A$ qualquer, $x \sim y$ se, e somente se $f(x) = f(y)$
   b) $x, y \in \mathbb{Z}$, dado um $n \in \mathbb{Z}$, $x \sim y$ se, e somente se $x - y$ é múltiplo de n denotado por $x \overset{n}{\equiv} y$ (x é côngruo módulo n a y).
2) Fazer exercícios 8 e 9, pág.13 do [GON].
3) Considere a relação de equivalência do exercício 1 letra b. Determine para $n = 2$ a classe de equivalência de zero e um. Faça o mesmo para $n = 6$.
4) Considere uma função $f : A \longrightarrow B$ sobrejetiva, e a seguinte relação de equivalência em A, $x \sim y$ se, e somente se $f(x) = f(y)$. Defina uma nova $g : A/\sim \longrightarrow B$ da seguinte forma: $g(\bar{a}) = f(a)$. Verifique que por construção g é injetiva, e portanto bijetiva.
5) Defina em $\mathbb{R}^2$ a seguinte relação de equivalência: $(x, y) \sim (a, b)$ se, e somente se $x = \pm a$.
   a) Prove que "$\sim$" é uma relação de equivalência.
   b) Calcule a classe de equivalência de $(1, 0)$.
   c) Descreva o espaço quociente $\mathbb{R}^2/\sim$.
6) Considere a relação em $\mathbb{Z}$: $a \sim b$ se, e somente se $|a| = |b|$.
   a) Mostre que é de equivalência.
   b) Determine as classes.
   c) Descreva $\mathbb{Z}/\sim$.
7) Considere em $\mathbb{N} \times \mathbb{N}$ a relação $(a, b) \sim (a, d)$ se, e somente se $a + d = b + c$.
   a) Mostre que é de equivalência.
   b) Defina a soma e produto como:
   $(a, b) +' (c, d) = (a + b, c + d)$
   $(a, b) *' (c, d) = (a * c + b * d, a * d + b * c)$
   Mostre que o quociente $(\mathbb{N} \times \mathbb{N})/\sim$ é isomorfo ao domínio $\mathbb{Z}$ com as operações acima.

V – Anel, Domínio, Corpo, Polinômio

Começaremos falando sobre as semelhanças e diferenças entre anel, domínio, corpo.

Estas estruturas algébricas consistem de um conjunto A munido de duas operações que respeitam algumas propriedades. São estas propriedades que distinguirão uma estrutura da outra. Os conjuntos não precisam ser números, podendo ser matrizes, polinômios, funções etc., contanto que as duas operações definidas nos mesmos respeitem as propriedades.

Por analogia com os inteiros normalmente uma operação é chamada de soma outra produto, mas não deixe que isto o induza a pensar na "soma" e "produto" de números exclusivamente, embora sirva de referência concreta. Eventualmente a soma pode ser uma rotação no espaço etc.

As estruturas foram criadas porque se demonstrarmos um teorema para anéis automaticamente tudo que for anel terá esta propriedade, não sendo necessário redemonstrar caso a caso.

Exemplo: Veremos que a existência de MDC e fatoração nos inteiros e nos polinômios decorrem destes serem Domínios Euclidianos (mais tarde veremos o que é isto), e não de qualquer outra característica peculiar.

Formalmente temos $(A, +, *)$ uma estrutura algébrica, onde "$+$" e "$*$" são operações binárias em A, ou seja, associam a cada dois elementos de A um outro:

$$+ : A \times A \longrightarrow A$$

$$* : A \times A \longrightarrow A$$

Para que um conjunto vire um Anel, Domínio ou Corpo, devemos definir as duas operações de forma adequada e a seguir demonstrar que de fato todas as propriedades valem.

Definição: ANEL – Procure todas as propriedades em qualquer livro de Álgebra, e lembre-se que é uma estrutura onde a soma é bem comportada (tem neutro, inverso, associativa, é comutativa) e a multiplicação somente é associativa. Temos também a única propriedade que relaciona ambas: a distributividade. Um anel comutativo é uma anel onde a multiplicação é comutativa. Um anel com identidade é um anel que possui o elemento neutro (o "1") da multiplicação.

Definição: DOMÍNIO DE INTEGRIDADE – É anel comutativo, com identidade e (fato mais importante !) sem divisores de zero, que quer dizer que se $a * b = 0$ então $a = 0$ ou $b = 0$.

Definição: CORPO – É anel comutativo com identidade e que possui inverso multiplicativo, ou seja, $\forall a \in K$, $a \neq 0$, $\exists a^{-1} \in K$; $a * a^{-1} = 1$.

Como exemplos destes objetos temos em primeiro lugar os conjuntos numéricos. $\mathbb{N}$ não é sequer anel, pois não possui elemento inverso para adição. $\mathbb{Z}$ é um anel comutativo, na realidade mais do que isto, é um domínio de integridade, pois não possui divisores de zero. $\mathbb{Q}$, $\mathbb{R}$, e $\mathbb{C}$ são exemplos de anéis, domínios e corpos. Deve estar claro que todo corpo é domínio de integridade e todo domínio é anel.

Como outro exemplo de anel temos o conjunto das matrizes quadradas com soma e produto usuais. Não é domínio pois possui divisores de zero (verifique !).

Exercícios:

1) Prove que num anel a lei do corte ($a * b = a * c$ implica que $b = c$) é equivalente a não existência de divisores de zero.
2) Prove que num anel comutativo com unidade a existência de inverso multiplicativo implica na não existência de divisores de zero. Conclua que todo corpo é domínio de integridade.
3) Seja D um Domínio de Integridade. Prove que as únicas soluções de $x^2 = x$ são $x = 0$ ou $x = 1$.
4) Faça, do livro [GON], pág.40, os exercícios 7,8,9,10,14,15,16,18.

Definição: POLINÔMIOS – Dado um anel A definimos um novo conjunto denotado por $A[x]$ (um mero símbolo) para indicar o conjunto de polinômios $f(x)$ com coeficientes em A. Estes polinômios serão "coisas" da forma $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Podemos ver um polinômio sem os x's assim $(a_0, a_1, \cdots, a_{n-1}, a_n)$, como uma sucessão ordenada de coeficientes, tal qual as coordenadas de um vetor em Álgebra linear.

Exemplo: Um vetor em $\mathbb{R}^3$ pode ser denotado por $(3, 4, 5)$, ou $3e_1 + 4e_2 + 5e_3$ ou $3i + 4j + 5k = 4j + 3i + 5k$. A importância das letras ao lado dos números — neste exemplo, i, j, k, e_1, e_2, e_3 ; no caso de polinômios $x, x^2, \ldots, x^n$ — é para se recuperar os coeficientes de forma ordenada quando for necessário.

Neste ponto não nos interessa ainda substituir os x's por números, $f(x)$ é uma mera expressão formal. Quando queremos substituir x por um número e verificar quanto vale $f(x)$ estaremos lidando com uma função polinomial. De fato polinômios e funções polinomiais apresentam uma relação importantíssima, que veremos mais adiante.

Exemplo: No anel $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ o polinômio em $\mathbb{Z}_2[x]$ $f(x) = \bar{1}x^2 + \bar{1}x$ não é nulo, porém como função polinomial, $f(x)$ é sempre zero (verifique !).

Agora que definimos o conjunto $A[x]$, resta definir a soma e o produto de dois elementos deste conjunto, ou seja, dois polinômios. Leia a definição em qualquer livro de Álgebra, e preste atenção que a soma e o produto de polinômios é definida através da soma e produto no anel A. Desta forma é imediato verificar que $(A[x], +', *')$ é anel ($+'$ e $*'$ em contraste com $+$ e $*$ do anel A). Leia também a definição de grau de um polinômio, denotado por grau$(f(x))$.

Exercícios:

1) Mostre que as matrizes reais da forma $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ relativamente a soma e produto usual de matrizes forma um anel. Este anel não possui unidade à direita, no entanto possui uma infinidade de unidades à esquerda da forma: $\begin{pmatrix} 1 & t \\ 0 & 0 \end{pmatrix}$
2) Verifique que o conjunto de matrizes com coeficientes em $\mathbb{Z}$, com a soma e produto usuais de matrizes, é um anel.
3) Mostre que se $f(x), g(x) \neq 0 \in D[x], D$ um domínio de integridade, grau$(f(x) * g(x))$ = grau $f(x)$ + grau $g(x)$.

VI – Tópicos em Anéis

1) Introdução

Antes de começar não custa lembrar que estas definições valem para domínios e corpos, pois estes são anéis também. Um subanel de um anel A é um subconjunto de A que continue sendo um anel. O risco de um subconjunto não ser subanel é que ele não seja fechado para soma e produto, ou seja, $a, b \in B, a-b \notin B$ ou $a*b \notin B$. A definição que daremos a seguir é também o guia para se resolver todo exercício que peça para se verificar se um determinado subconjunto de A é subanel.

2) Subanel e Ideal

Definição: SUBANEL – Seja A uma anel, $B \subseteq A$, dizemos que B é subanel de A caso:

(i) $0 \in B$
(ii) $x, y \in B$ implica que $x - y \in B$
(iii) $x, y \in B$ implica que $x * y \in B$

Definição: IDEAL – Seja A um anel, $I \subseteq A$. Dizemos que I é ideal a esquerda de A caso:

(i) $0 \in I$
(ii) $x, y \in I$ implica que $x - y \in I$
(iii) $a \in A, b \in I$ implica que $a * b \in I$

Definimos um ideal a direita de A de forma análoga. Deve-se notar que a diferença entre subanel e ideal é quanto ao fechamento da multiplicação. Enquanto no subanel basta se verificar o fechamento entre elementos do subconjunto, no caso do ideal temos que verificá-lo entre todos os elementos do anel vezes os elementos do ideal. Disto deve ficar claro que todo ideal é um subanel.

Exemplo: A forma mais natural de se gerar um ideal é pegar um $a \in A$ e definir $I = \{a * x; \forall x \in A\}$. Denotamos $I = (a)$, e dizemos que o ideal I é gerado por a.

Obs1: Cuidado que quando falamos em ANEL não estamos assumindo que a multiplicação seja comutativa. Por isto temos ideais a esquerda e a direita de A. Na resolução de exercícios seja cuidadoso com isto.

Obs2: Para demonstrar que algum conjunto é um ideal, ajuda chamá-lo de outra letra, J por exemplo, e escrever as propriedades que tem que valer para J. Desta forma evitam-se tropeços, pois na propriedade de fechamento pela multiplicação por elemento do anel, um está no ideal, outro no anel. Cuidado !!!

Obs3: Um ideal é como um subespaço vetorial, tendo muitas características interessantes como ser gerados por alguns elementos do anel, tal qual um subespaço (Veremos isto no exercício 6 abaixo !).

Exercícios:

1) Assuma que I_n é ideal para todo n. Prove que são ideais:
   a) $I_1 \cap I_2 \cap \cdots \cap I_n$
   b) $I_1 + I_2 + \cdots + I_n = \{x_1 + x_2 + \cdots + x_n; x_j \in I_j\}$
2) Prove que se A é um anel com identidade 1, e $I \subset A$ ideal, $1 \in I$ implica que $I = A$.
3) Seja I um ideal de A. Mostre que se para $x, y \in A$ definirmos $x \sim y$ se, e somente se $x - y \in I$ é uma relação de equivalência em A.
4) Sejam $a\mathbb{Z}$ e $b\mathbb{Z}$ ideais de $\mathbb{Z}$ com $a\mathbb{Z} \subseteq b\mathbb{Z}$. Prove que b divide a.
5) Assuma que $a\mathbb{Z} = b\mathbb{Z}$. Prove que $a = b$ ou $a = -b$.
6) Prove que o conjunto $I = (a)$ definido no exemplo é de fato um ideal. Mais geralmente assuma que $a_1, \ldots, a_n \in A$, mostre que $I = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n; x_1, \ldots, x_n \in A\}$ é um ideal. Este ideal é denotado por $I = (a_1, a_2, \ldots, a_n)$.

Obs: O ideal do exercício 6) é formado pela combinação linear de coeficientes. Fazendo analogia com álgebra linear, dado um conjunto de vetores, a combinação linear destes determina um subespaço vetorial.

3) Anel Quociente

O resumo do que faremos é que, dado um anel A qualquer e um ideal $I \subseteq A$, podemos definir um novo conjunto A/I e novas operações neste conjunto de modo que tenhamos um outro anel. O roteiro do nosso procedimento é:

a) Definir a relação de equivalência do exercício 4) anterior, $x \sim y$ se, e somente se $x - y \in I$.

b) Denotar A quociente pela relação acima, por $A/I = A/\sim$. Este conjunto novo é o conjunto do anel quociente.

c) Definir as novas operações em A/I para que vire um anel.

Exemplo: Seja $A = \mathbb{Z}$, e $I = 3\mathbb{Z}$. $A/I = \{\bar{0}, \bar{1}, \bar{2}\}$

Pelo resumo fica imediato quem é o novo conjunto. Resta definir novas operações neste, operações estas induzidas pelas operações no anel A.

Definiremos $\bar{a}, \bar{b} \in A/I$, $\bar{a} +' \bar{b} = \overline{a+b}$. Ou seja para somar duas classes de equivalência tomamos dois representantes quaisquer em A/I destas classes, somamos em A, e tomamos a classe da soma. A definição para o produto é inteiramente análoga.

Exercícios:

1) Verifique se as operações estão bem definidas, isto é, tomando qualquer representante o resultado é o mesmo. Você tem que verificar se tomando $\bar{a} = \bar{b}$, e $\bar{c} = \bar{d}$ implica que $\bar{a} +' \bar{b} = \bar{c} +' \bar{d}$ (análogo para o produto).
2) Verifique que no anel quociente A/I a classe de $a \in A$ é a mesma do zero se, e somente se $a \in I$; ou seja, $\bar{a} = \bar{0}$ se, e somente se $a \in I$. Quando passamos o quociente os elementos do ideal viram o zero do anel quociente.

Agora que temos o conjunto A/I, duas operações bem definidas, resta verificar se satisfaz as propriedades de anel. Não farei a verificação, porém, pela forma como definimos a soma e o produto, esta é imediata, decorrendo do fato de A ser anel.

Finalmente podemos afirmar que dado um anel A qualquer e um ideal $I \subseteq A$ podemos construir $(A/I, +', *')$, chamado anel quociente de A por I.

Obs1: Uma analogia possível é que dado um espaço vetorial V, $T : V \longrightarrow V$ linear, $\ker(T)$ é um subespaço vetorial e podemos definir de forma análoga $V/\ker(T)$ um espaço vetorial quociente.

Obs2: Notações:

- $3\mathbb{Z} = \{3a; a \in \mathbb{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$ = Ideal gerado por 3.
- $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ = Anel quociente $\mathbb{Z}$ pelo ideal $3\mathbb{Z}$

Obs3: Logo $n\mathbb{Z} \neq \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. O primeiro é o ideal gerado por n, o segundo é um anel quociente. $\mathbb{Z}_n$ possui n elementos, enquanto $n\mathbb{Z}$ possui infinitos elementos. A soma de elementos de $n\mathbb{Z}$ é a mesma em $\mathbb{Z}$ (a "normal"), enquanto em $\mathbb{Z}_n$ é a soma módulo n.

Abaixo vem uma série de exercícios que aplicam os anéis $\mathbb{Z}_n$. Espero que motivem o aprendizado e uso dos mesmos.

Exercícios:

1) Procure os elementos invertíveis em $\mathbb{Z}_{12}$ e em $\mathbb{Z}_7$. Qual a diferença ? Porque ? Enuncie (e prove) um teorema com sua conclusão.
2) Prove que são irracionais: $\sqrt{3}$, $\sqrt[3]{2}$, $\sqrt[3]{9}$, $\sqrt{21}$, $\sqrt[5]{16}$ e $\sqrt{30}$.
3) Generalize o exercício anterior provando que dado um $p \in \mathbb{N}$ primo e $n > 1$ são irracionais: $\sqrt[n]{p}$ e $\sqrt[n]{p^m}$ (com $0 < m < n$).
4) Generalize o exercício anterior provando que dados $p_i \in \mathbb{N}$ primos distintos entre si são irracionais: $\sqrt[n]{p_1p_2\cdots p_k}$ $(n > 1)$ e $\sqrt[n]{p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}$ (se $a_k \bmod n \neq 0$ para pelo menos um k).
5) Lembra-se da prova dos nove ? É o seguinte: você faz uma soma de $a + b = c$, números inteiros grandes, e quer verificar se o resultado está correto. Some todos os algarismos de a e b com resto módulo 9 (em $\mathbb{Z}_9$) e verifique se a soma de todos os algarismos de c dá o mesmo resultado. Para checar o produto some todos os algarismos de a com resto mod 9 e multiplique pela soma mod 9 de b. O resultado mod 9 tem que ser a soma dos algarismos de c mod 9. Prove porque funciona. Por exemplo:

$$\begin{array}{rlcccl} 1759 & 1+7+5+9 & = & 22 & \overset{9}{\equiv} & 4 \\ +\underline{3877} & 3+8+7+7 & = & 25 & \overset{9}{\equiv} & \underline{+7} \\ 5636 & 5+6+3+6 & = & 20 & \overset{9}{\equiv} & 11 \overset{9}{\equiv} 2 \end{array}$$

$$\begin{array}{rrcccl} 1329 & 1+3+2+9 & = & 15 & \overset{9}{\equiv} & 6 \\ \underline{\times 88} & 8+8 & = & 16 & \overset{9}{\equiv} & \underline{\times 7} \\ 116952 & 1+1+6+9+5+2 & = & 24 & \overset{9}{\equiv} & 42 \overset{9}{\equiv} 6 \end{array}$$

6) Sejam $a_1, a_2, \ldots, a_n$, "n" números naturais diferentes de zero. Prove que é possível escolher um subconjunto destes números de modo que a soma deles seja divisível por "n". Dica: Utilizando a barra para denotar congruência módulo "n", denote $b_1 = \overline{a_1}, b_2 = \overline{a_1 + a_2}, b_k = \overline{\sum_{i=1}^{k} a_i}$. Mostre que $b_i = b_j$ para $i \neq j$ implica na existência de subseqüência de números naturais com soma divisível por zero. Caso todos b_i's sejam distintos mostre que existirão "n" classes e que uma delas terá que ser zero.

7) Aprendemos no colégio alguns critérios de divisibilidade. Gostaria de aplicar a teoria aprendida sobre os $\mathbb{Z}_n$ para se demonstrar a validade dos critérios. Vou enunciá-los e o exercício consiste em demonstrar a validade. Em todos os enunciados utilizo a notação $a = \sum_{i=0}^{N} a_i 10^i, 0 \leq a_i \leq 9$. Ex: $125 = 5 \cdot 10 + 2 \cdot 10 + 1 \cdot 10$. Nesta notação a_0 é o último dígito.
   a) Div 2: Se a_0 é par (ou $a_0 \bmod 2 = 0$).
   b) Div 3: Se $\sum_i a_i \bmod 3 = 0$.
   c) Div 4: Se o número formado pelos dois últimos dígitos $(a_1 a_0)$ for divisível por 4.
   e) Div 5: Se termina em zero ou cinco.
   c) Div 8: Se o número formado pelos três últimos dígitos $(a_2 a_1 a_0)$ for divisível por 8.
   d) Div 9: Se $\sum_i a_i \bmod 9 = 0$.
   e) Div 10: Se termina em zero.
   f) Div 11: Se a soma $a_0 - a_1 + a_2 - a_3 \cdot = \sum_i (-1)^i a_i \bmod 11 = 0$.
8) Existe um critério simples para divisibilidade por 7 ? Porque ? E para 16 ?

4) Homomorfismo e Isomorfismo

Estes conceitos são muito importantes, na realidade tendo um papel fundamental na Matemática. Literalmente ISOMORFISMO quer dizer "*aquele que tem ou apresenta a mesma forma*".

Começaremos com uma analogia para entender o que é homomorfismo. Suponha que temos um conjunto de ovelhas (chamaremos de O) e o conjunto N dos números naturais. Agora definimos a operação de agrupamento no conjunto O como a junção de um conjunto de ovelhas com o outro.

Agora verificamos que somar em N é uma operação fácil de ser realizada. Por outro lado ir para uma fazenda e tentar reunir um conjunto de ovelhas com outro (mesmo com a ajuda de um cão pastor !) é uma tarefa bastante penosa, que além do esforço físico toma bastante tempo. Na prática diária fazemos o seguinte:

(i) Identificamos uma ovelha com o número 1.

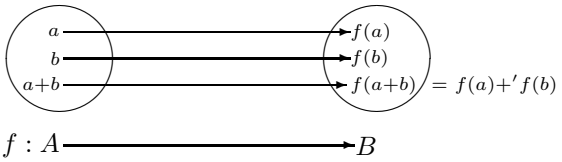
(ii) Identificamos duas ovelhas com o número 2, e assim sucessivamente ...

(iii) Quando queremos agrupar ovelhas transformamos em números, somamos em N, e retornamos para o conjunto de ovelhas sem ter que sair do lugar !

Exemplo: Uma outra analogia para homomorfismo. Temos um conjunto de bananas e outro de maças. Suponha que sabemos somar bananas mas não sabemos somar maçãs. Agora nos pedem para fazer uma conta em maçãs. Caso tivéssemos uma f relacionando um conjunto ao outro que preservasse as operações levaríamos as maçãs para o conjunto de bananas, faríamos as contas lá, e devolveríamos em maçãs a resposta.

Formalizando, um homomorfismo entre anéis é uma função $f : A \longrightarrow B$, que preserva a soma e o produto. Quero dizer que somar dois elementos em A e levar para B é o mesmo que levar os elementos de A para B e somar em B. O mesmo deve ocorrer com o produto (observe a figura abaixo). Deve ficar claro que a soma e o produto de A são diferentes da soma e produto em B.

Definição: HOMOMORFISMO – Dados $(A, +, *)$, $(B, +', *')$ anéis, uma $f : A \longrightarrow B$ é homomorfismo quando $\forall a, b \in A;\ f(a+b) = f(a) +' f(b)$ e $f(a * b) = f(a) *' f(b)$.



Obs: Para mostrar que f é um homomorfismo basta mostrar que f respeita a soma/produto como acima, f não precisa ser injetiva nem sobrejetiva.

Exemplo1: $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ dado por $f(x) = x \bmod n = \bar{x}$

Exemplo2: A, B anéis quaisquer, $f : A \longrightarrow B$, $f(x) = 0, \forall x \in A$.

Exercícios:
1) Sejam A, B anéis. $f : A \longrightarrow B$ um homomorfismo. Prove que:
   a) $\ker f = \{a \in A;\ f(a) = 0\}$ é um ideal.
   b) $\mathrm{Im} f = \{f(a);\ a \in A\}$ é subanel de B.
   c) f é injetiva se, e somente se $\ker f = \{0\}$
2) Sejam A e A' anéis, $f : A \longrightarrow A'$ homomorfismo. Prove que:
   a) $f(0) = 0'$
   b) $f(-a) = -f(a);\ \forall a \in A$.
3) Seja $f : A \longrightarrow B$ um homomorfismo de anéis, $I = \ker(f)$. Prove que $f(x) = f(y)$ se, e somente se $x - y \in I$. Portanto é a mesma coisa definir $x \sim y$ de qualquer uma das duas formas anteriores.
4) Seja K um corpo. Mostre que todo ideal de K é trivial, ou seja, ou é $\{0\}$ ou o próprio K.

Obs: Deve ficar clara a analogia com Álgebra linear, onde o núcleo de uma transformação linear é sempre um subespaço vetorial, e a T.L. é injetiva se, e só se, o núcleo = (0) (vide Exercício 1 acima).

Definição: ISOMORFISMO – É um homomorfismo bijetivo, ou seja, uma função f que seja homomorfismo, f uma bijeção, significa dizer que f é um isomorfismo.

Exercício: Mostre que se f é homomorfismo, $f : A \longrightarrow B$ é bijetiva, f^{-1} é homomorfismo $f^{-1} : B \longrightarrow A$.

Pelo exercício anterior, quando temos um isomorfismo temos um homomorfismo de A em B, e de B em A. Para perceber a importância podemos voltar ao exemplo das ovelhas e de N. Na realidade temos um isomorfismo. Toda vez que nos derem um problema em ovelhas transformamos em números, fazemos as contas, e devolvemos a resposta em ovelhas.

De modo geral, supondo que seja mais fácil operar num conjunto do que em um outro, tendo um isomorfismo entre eles podemos pela f (ou f^{-1}) trazer o problema para o conjunto fácil, operar, e devolver a resposta onde quiser.

Exemplo: A operação de soma em $\mathbb{R}$, e produto em $\mathbb{R}^*$. Somar é muito mais fácil do que multiplicar, e temos de fato uma $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ bijetiva que satisfaça $f(a \times b) = f(a) + f(b)$.

Deve-se notar que $f(x) = \log(x)$ é tal função. Este, aliás, é o princípio da régua de cálculo, onde toda vez que temos que multiplicar diversos números tomamos seus log's, somamos, e aplicamos $\log^{-1}$ para obter a resposta.

Quando estabelecemos um isomorfismo entre duas estruturas (neste caso anéis) dizemos que estas estruturas são iguais, idênticas, ou a mesma a menos de um isomorfismo. Ou diretamente, as estruturas são isomorfas. Denota-se $A \simeq B$ para dizer que A e B são isomorfos.

Exemplo: Já sabemos o que é um corpo, um conjunto ordenado a maioria deve saber, e completo, quem já viu análise sabe. É possível demonstrar que a menos de um isomorfismo existe um único corpo ordenado completo, $\mathbb{R}$. Qualquer outro será isomorfo a este.

Definição: ENDOMORFISMO – Homomorfismo de um anel nele mesmo.

Definição: AUTOMORFISMO – Isomorfismo de um anel nele mesmo.

Exemplo1: A função $I : A \longrightarrow A$, $I(x) = x$ para todo $x \in A$ (função Identidade) é um automorfismo de A em A.

Exemplo2: $f : \mathbb{C} \longrightarrow \mathbb{C}$; $f(z) = \bar{z}$ (conjugado complexo) é um automorfismo de $\mathbb{C}$ (Verifique !).

Exercícios:

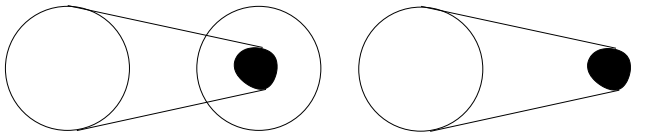
1) Assuma que $f(x) \in K[x]$. Verifique que é necessário que φ seja um homomorfismo e que para todo $a \in K$, $\varphi(a) = a$ para que $\varphi(f(x)) = f(\varphi(x))$.
2) Considere f:$\mathbb{Z} \longrightarrow \mathbb{Z}$ dada por f(n) = 3n. Verifique se f é endomorfismo do anel $\mathbb{Z}$.
3) Considere o anel $\mathbb{Z}[\sqrt{2}]$. Este anel tem elemento neutro da multiplicação ? Considere $f(a + b\sqrt{2}) = ab\sqrt{2}$. f é automorfismo ?
4) Faça [GON] pág. 59, ex. 10.

5) Teorema do Homomorfismo

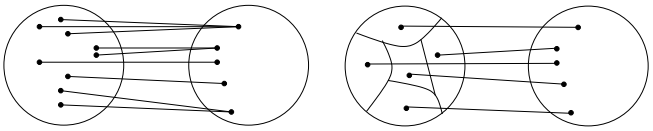
Antes de enunciar este teorema vamos fazer um roteiro do que desejamos fazer. Começando com um homomorfismo $f : A \longrightarrow B$ queremos chegar a um isomorfismo.

I) A função f deve tornar-se bijetiva

a) Caso f não seja sobrejetiva, façamos o processo que ensinamos acima, ou seja, restringir o contradomínio à imagem, transformando em $f : A \longrightarrow \mathrm{Im}(f)$.



b) Caso f não seja injetiva faça o processo de torná-la injetiva definindo o novo conjunto de classe de equivalência de A, onde $x, y \in A, x \sim y$ se, e somente se $f(x) = f(y)$ (ou se, e somente se $x - y \in \ker(f)$). Chamando $\ker(f) = I$; $\bar{f} : A/I \longrightarrow B$ será injetiva, onde A/I é o anel quociente de A.



II) Agora que $\bar{f}$ é sobrejetiva, temos que verificar se é homomorfismo do anel A/I em $\mathrm{Im}(f)$.

III) Finalmente, A/I e $\mathrm{Im}(f)$ são anéis, $\bar{f}$ é homomorfismo bijetivo, e portanto um isomorfismo.

Teorema Dados A, B anéis, $f : A \longrightarrow B$ homomorfismo, $I = \ker(f)$, então A/I é isomorfo a $\mathrm{Im}(f)$, ou seja, $A/I \simeq \mathrm{Im}(f)$.
Dem.: Está acima.

Obs: Para este teorema ser melhor entendido faremos novamente uma analogia com álgebra linear. Seja $T : V \longrightarrow V$ uma transformação linear. Temos que $\ker(T)$ é subespaço vetorial. Podemos definir, conforme já dissemos, o espaço vetorial quociente $V/\ker(T)$. Também temos que $V/\ker(T)$ é isomorfo a $\mathrm{Im}(T)$. Para que dois espaços vetoriais sejam isomorfos eles tem que possuir a mesma dimensão. Temos portanto que $\dim(V/\ker(T)) = \dim(\mathrm{Im}(T))$. Pelo teorema do núcleo-imagem (Álgebra Linear) calculamos que $\dim(V/\ker(T)) = \dim(\mathrm{Im}(T)) = \dim(V) - \dim(\ker(T))$.

6) Tipos de Ideais

Definição: Ideal MAXIMAL – Um $M \subsetneq A$ é maximal se, e somente se não existe J tal que $M \subsetneq J \subsetneq A$.

Um ideal maximal é tal que não existe um ideal que esteja contido propriamente entre este e o anel. Outra forma de se ver é que caso tentemos aumentar um ideal para obtermos outro ideal um pouco maior obtemos todo o anel.

Exemplo: $7\mathbb{Z}$ é maximal em $\mathbb{Z}$. Por outro lado $8\mathbb{Z}$ não é maximal em $\mathbb{Z}$ pois temos $8\mathbb{Z} \subsetneq 4\mathbb{Z} \subsetneq \mathbb{Z}$.

Definição: Ideal PRINCIPAL – $I \subseteq A$ é principal se, e somente se I pode ser gerado por um único elemento do anel, ou seja, $\exists a \in A, I = (a)$.

Exemplo: $A = \mathbb{Z}[x], I = 2A + xA$ (gerado por 2 e x) não é principal.

Lema Seja M um ideal, A um anel comutativo com unidade. Então, M é um ideal maximal se, e somente se A/M é corpo.
Dem.: ($\Longrightarrow$) Considere o ideal $J = \{ra + m; r \in A, m \in M\}$, onde $a \notin M$. Queremos mostrar agora que todo $a \neq 0 \in A/M$ tem inverso.

a) Temos que verificar se J é de fato um ideal, porém isto será deixado como exercício. Dica $J = (a) + M$.

b) Temos claramente que $M \subset J$, no entanto, como $a \notin M, M \neq J$. Portanto temos, $M \subsetneq J \subset A$. Como M é maximal, $J = A$.

c) Como $J = A, 1 \in A$ implica que $1 \in J$. Portanto, $\exists b \in A, \exists m \in M, 1 = ba + m$. Passando a barra em ambos os lados, temos que $\bar{1} = \bar{b}\bar{a}$, ou seja, $\bar{b}$ é o inverso de $\bar{a}$.

d) Portanto como A é anel quociente de um anel comutativo com unidade, A/M é anel comutativo com unidade onde todo elemento não nulo tem inverso, ou seja, é um corpo.

($\Longleftarrow$) Seja $f : A \longrightarrow A/M$ o homomorfismo natural que associa a cada elemento do anel sua classe de equivalência. Seja $J \subset A$ um ideal de A.

a) $f(J)$ é um ideal em A/M (fica como exercício !).

b) Como A/M é corpo, $f(J) = \{0\}$ ou $f(J) = A/M$.

c) Caso $f(J) = \{0\}, a \in J$ implica que $a \sim 0$ se, e somente se $a - 0 \in M$ se, e somente se $a \in M$. Ou seja, $J = M$.

d) Caso $f(J) = A/M$, como $\bar{1} \in A/M, 1 \in J$. Isto implica que $J = A$. ■

Exercícios:
1) Fazer exercícios 2, 3, 4, 16 e 20, pág.39 do [GON].
2) Fazer exercícios 1, 4, 5 e 6, pág.45 do [GON].

VII – Domínios Euclidianos

1) Introdução

Estamos interessados neste trabalho principalmente nos domínios $\mathbb{Z}$ e $K[x]$, ou seja, nos inteiros e nos polinômios de um corpo, principalmente $\mathbb{Q}$ ou $\mathbb{R}$. Na parte de irredutibilidade de polinômios trabalharemos com $\mathbb{Z}[x]$ também. Apesar de trabalharmos quase exclusivamente com estes dois objetos, gostaria de explicar porque introduzo o conceito de domínios euclidianos. Em primeiro lugar porque será importante no prosseguimento do aprendizado de álgebra e, principalmente, porque demonstraremos logo abaixo diversos teoremas cujas demonstrações valem basicamente por causa da existência do algoritmo de divisão de Euclides, e não por outro fato qualquer.

2) Definições

Um domínio euclidiano é um domínio de integridade em que existe o algoritmo da divisão de Euclides. Para isto precisamos de uma função $\varphi : D \setminus \{0\} \longrightarrow \mathbb{N}$ que medirá o "tamanho" do resto. No caso dos inteiros $\mathbb{Z}$ esta função será o módulo, $\varphi(x) = |x|$. No caso dos polinômios a função será o grau do polinômio, $\varphi(f(x)) = \text{grau}(f(x))$.

Definição: DOMÍNIO EUCLIDIANO – Seja D um domínio de integridade e $\varphi : D \setminus \{0\} \longrightarrow \mathbb{N}$ em que: $\forall a, b \in D, b \neq 0$, existe q e $r \in D$ tal que $a = b * q + r$, com $\varphi(r) < \varphi(q)$ ou $r = 0$.

Agora teríamos que verificar que $\mathbb{Z}$ e $K[x]$ são de fato domínios euclidianos, entretanto recomendamos que o leitor recorra ao [GON] para ver a demonstração.

Obs1: Daqui por diante começaremos a demonstrar teoremas importantes para domínios euclidianos, alertas que temos em mente neste curso $\mathbb{Z}$ e $\mathbb{R}[x]$. No entanto, sabemos que são válidos para $\mathbb{Z}[i]$ e outros domínios euclidianos.

Obs2: $\mathbb{Z}[i]$ é domínio euclidiano com a seguinte função, seja $a + bi \in \mathbb{Z}[i], \varphi(a + bi) = a^2 + b^2$.

Obs3: Qualquer corpo vira um domínio euclidiano com a função $\varphi(x) \equiv 0$ pois a divisão num corpo é exata (o resto é sempre zero !).

Exercício: Mostre que $\mathbb{Z}[x]$ não é domínio euclidiano com a função grau. Dica: Tente dividir um polinômio por uma constante.

3) Domínio Principal

Demonstraremos agora o fato de todo domínio euclidiano ser um domínio de ideais principais. Daqui decorre que sempre que dermos um $I \subset D$ domínio principal, podemos escrever $I = (a)$ para algum $a \in D$. Na demonstração fica clara a importância fundamental da existência do algoritmo de Euclides.

Teorema Para todo ideal $I \subset D$ um domínio euclidiano, $\exists a \in D, I = (a)$.

Dem.:

a) Defina o conjunto $B \subset N$ por $B = \text{Im}(\varphi) = \varphi(I \setminus \{0\})$.

b) Obviamente todo subconjunto de N possui menor elemento, logo para $B \subset N$, existe um b menor elemento de B.

c) Considere um $a \in I$ tal que $\varphi(a) = b$ (pode não ser único, qualquer um serve !).

d) Agora mostraremos que $I = (a)$, ou seja, a gera todo o ideal. Para isto considere um $x \in I$. Podemos utilizar o algoritmo de Euclides e dividir x por a. Deste modo $x = a * q + r$, com $\varphi(r) < \varphi(a)$ ou $r = 0, q, r \in D$.

e) Afirmo que $r \in I$, pois $r = x - a * q$ e temos o fechamento da soma/produto do ideal.

f) Sabendo que $r \in I$, temos por outro lado que $r = 0$ ou $\varphi(r) < \varphi(a)$. Porém $\varphi(a)$ foi escolhido o menor possível, o que implica que $r = 0$.

g) Resumindo, $\forall x \in I$, $\exists a \in I$, $x = a * q + 0$, $q \in D$. Portanto $I = (a) = aD$ ■

4) Existência do MDC

O importante conceito de MDC será introduzido aqui de uma forma que possa ser generalizado para outros domínios que não sejam os números inteiros. Para isto será necessário repensá-lo na linguagem de ideais.

Embora a definição aqui possa parecer mais pedante, veremos que o MDC de um conjunto finito de elementos de um domínio euclidiano será tal que $\text{MDC}\{a_1, \ldots, a_n\} = d$:

i) d divide cada elemento a_i

ii) Caso exista outro elemento d' que divida cada a_i, d' dividirá d, o que podemos entender em $\mathbb{Z}$ como $|d'| < |d|$, ou seja, ele é o maior entre os divisores.

Com d satisfazendo i) e ii) justifica-se que se diga que ele é o MDC (maior divisor comum). Necessitaremos da linguagem de ideais para demonstrar que ele (d) sempre existe em um domínio euclidiano.

Teorema (Existência do MDC) Seja D um domínio euclidiano, $I = a_1D + a_2D + \cdots + a_nD$. Teremos que:

i) $\exists d \in D$, $I = (d) = dD$.

ii) $d|a_i$; $\forall i \in \{1, \ldots, n\}$

iii) Caso $\exists d' \in D$; $d'|a_i$; $\forall i \in \{1, \ldots, n\}$; $d'|d$.

iv) $\exists r_1, r_2, \ldots, r_n \in D$; $d = a_1r_1 + \cdots + a_nr_n$

Dem.:

i) Já foi provado que todo ideal $I \subset D$ pode ser gerado por um $d \in D$.

ii) Para cada i, $a_iD \subset I = (d)$ implica que $d|a_i$. Observe que quando somamos os ideais obtemos mais do que a simples união dos conjuntos.

iii) Como $d'|a_i$; $a_iD \subseteq d'D$. Temos portanto que cada ideal que somamos está contido no ideal $d'D$. A soma deles, que é I, esta contido em $d'D$, ou, $I = (d) = dD \subseteq d'D$ implica que $d'|d$.

iv) Pela definição de soma de ideais isto é imediato. ■

Obs1: Se $1 = ab+cd$ em $\mathbb{Z}$ então $\text{MDC}(a,c) = \text{MDC}(b,d) = \text{MDC}(a,d) = \text{MDC}(b,c) = 1$. Isto é verdade pois tomando $I = a\mathbb{Z} + c\mathbb{Z}$, $\exists b, d \in \mathbb{Z}$, $ab + cd = 1$. Logo $1 \in I$ e portando $I = \mathbb{Z} = (1)$. Logo $\text{MDC}(a,c) = 1$. Os outros casos são análogos.

Obs2: Isto não é verdade para qualquer elemento de $\mathbb{Z}$. $4 = ab + cd$ não implica que $\text{MDC}(a,c) = 4$. Exemplo: $4 = 8 \cdot 1 + 2 \cdot (-2)$ e $\text{MDC}(8,2) = 2$, e não 4.

5) Ideais Maximais e Primos

Em primeiro lugar vamos ver o que são elementos primos ou irredutíveis. Para isto precisamos de algumas definições:

Definição: INVERTÍVEL – Elemento $a \in D$ tal que existe um $b \in D$ satisfazendo $a * b = 1$.

Exemplo: Em $\mathbb{Z}$ os invertíveis são o 1 e o -1. Em $K[x]$ são os polinômios constantes, $f(x) = c, c \in K$.

Exercícios:

1) Mostre que caso os ideais I e $J \in \mathbb{R}[x]$ sejam iguais é porque os polinômios geradores de I e J diferem por um $a \in \mathbb{R}$, ou seja, $f(x) = ag(x)$, onde $f(x)$ e $g(x)$ geram respectivamente I e J.
2) Mostre que caso tenhamos $I = J \subset D$ domínio euclidiano, o gerador de I difere do gerador de J por um elemento invertível de D. Mais precisamente, seja $I = aD, J = bD$. $aD = bD$ se, e somente se a e b diferem por um invertível, ou seja, $a = ub$, u invertível.

Definição: IRREDUTÍVEL OU PRIMO – Um $a \in D \setminus \{0\}$ é irredutível quando:

(i) a não é invertível

(ii) a só possui fatoração trivial, i.e., $a = b * c$ implica que b ou c é invertível.

Exemplo: Em $\mathbb{Z}$ os irredutíveis são os números primos. Em $K[x], f(x) = x + c$, é sempre irredutível.

Em $K[x]$ os irredutíveis são um problema de modo geral bastante difícil de se determinar. Teremos uma seção inteira somente para determinar critérios de irredutibilidade de um polinômio.

Veremos mais adiante que $x^2 + 1$ é irredutível em $\mathbb{R}[x]$. No entanto ele é redutível em $\mathbb{C}[x]$ pois $x^2 + 1 = (x - i)(x + i)$, uma fatoração não trivial.

Obs1: Embora exista uma distinção entre irredutíveis e primos, aqui trataremos os conceitos como se fossem o mesmo, pois em domínios fatoriais (veja 6 abaixo) eles coincidem. Para maiores detalhes, consultar o [GAR], pág.28.

Obs2: Neste contexto de Primo = Irredutível, vale que p um primo (ou irredutível), $p|ab$ implica que $p|a$ ou $p|b$.

Agora que sabemos o que é um elemento irredutível provaremos um teorema que diz que todo ideal maximal é gerado por um elemento irredutível. Assim, todos os ideais maximais de $\mathbb{Z}$ são os gerados por números primos.

Teorema Considere $I = (p) \subset D$, com D um domínio euclidiano e $p \in D$. São equivalentes:

i) I é um ideal maximal.

ii) p é um elemento irredutível (ou primo) de D.

Dem.: (i $\Longrightarrow$ ii)

Seja $I = pD$. Temos que mostrar que p é irredutível (ou primo). p não é invertível, pois senão teríamos $I = pD = D$.

Agora caso possamos escrever $p = a * b$, teríamos que:

$I = pD \subset aD \subset D$. Como I é maximal, temos duas possibilidades.

- $aD = D \Longrightarrow a$ é invertível
- $aD = pD \Longrightarrow a$ e p diferem por um invertível, ou seja, b é invertível.

(ii $\Longrightarrow$ i)

Seja um ideal J, $I \subset J \subset D$. Temos que J é gerado por algum elemento de $D, J = (a)$. Temos portanto que $(p) \subset (a) \subset D$. Pela inclusão de ideais, temos que $a|p$, ou, $p = a * b$, $b \in D$. Como p é irredutível(ou primo), a é invertível ou b é invertível. Temos portanto dois casos:

- a é invertível $\Longrightarrow aD = D$
- b é invertível $\Longrightarrow pD = (a * b)D = a * (bD) = aD$. ■

Exercício: Como generalização de uma observação feita anteriormente seja p um primo em $\mathbb{Z}$ com $p = ab + cd$. Prove que $\text{MDC}(a,c) = p$ ou $\text{MDC}(a,c) = 1$. Dica: $I = a\mathbb{Z} + c\mathbb{Z}$, verifique que $p\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$. Como $p\mathbb{Z}$ é maximal, $I = \mathbb{Z}$ ou $I = p\mathbb{Z}$).

6) Domínio Fatorial

Um domínio fatorial é um domínio de integridade no qual todo elemento não invertível se escreve como um produto finito de irredutíveis ou primos. A menos de ordenação e multiplicação por invertíveis, a fatoração é única.

Exemplo: Em $\mathbb{Z}$ todo elemento pode ser fatorado como um produto de primos. Quando se fala que a fatoração é a menos de invertíveis é porque $6 = 2 * 3 = (-2) * (-3)$. No caso de polinômios $\mathbb{R}[x]$ os invertíveis são as constantes $c \in K$. $x^2 - 1 = (x + 1)(x - 1) = (5x - 5)(x/5 - 1/5)$. Aí também a fatoração é única, a menos de multiplicação por invertíveis (neste caso o número 5 !).

Teorema Se D um domínio euclidiano então D é um domínio fatorial.

Dem.: A demonstração é um pouco longa, sendo mais importante conhecer e saber aplicar este teorema. Para os leitores interessados, consultar [GAR], pág. 29. ■

Obs: Poderíamos provar também que $\mathbb{Z}[x]$, embora não sendo domínio euclidiano, é domínio fatorial. Para tal ver [GAR], pág.35.

VIII – Irredutibilidade em Polinômios

1) Introdução

Nesta seção aprenderemos algumas condições para se determinar a irredutibilidade de um polinômio. Veremos dois critérios (o Lema de Gauss e o do corpo finito) que transferem o estudo de irredutibilidade no corpo $\mathbb{Q}$ para o domínio $\mathbb{Z}$ ou para o corpo finito $\mathbb{Z}_p$. Temos ainda o de Eiseinstein e o das raízes.

Obs: Ao contrário do que fizemos no capítulo anterior, aqui trabalharemos com $\mathbb{Z}$ e $\mathbb{Q}$ diretamente, no entanto os teoremas e lemas abaixo funcionam igualmente para um domínio (ao invés de $\mathbb{Z}$) e seu corpo de frações (ao invés de $\mathbb{Q}$). A respeito de corpo de frações de um domínio ver apêndice 4.

Dado um domínio, podemos classificar seus elementos não-nulos como:

(i) Invertível: Elemento $u \in D, \exists u^{-1} \in D, u * u^{-1} = 1$.

(ii) Irredutível ou Primo: Elementos que só possuem fatoração trivial, isto é, $a = b * c, b$ ou c é invertível.

(iii) Fatorável: Elemento que possui fatoração não trivial, i.e., $a = b * c$, b e c não invertíveis.

Obs1: Um elemento não pode ser duas coisas ao mesmo tempo.

Obs2: Se todo elemento não-nulo do domínio é invertível então o domínio é um corpo.

Exemplo1: Em $\mathbb{Z}$ os invertíveis são: $\{1, -1\}$. Em $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ todos os elementos $\neq 0$ são invertíveis.

Exemplo2: Nos polinômios, todo polinômio de grau > 0 é não invertível (porque ?).

Exemplo3: Em $\mathbb{Z}[x]$ os invertíveis são $\{1, -1\}$ Em $K[x]$ os invertíveis são os polinômios constantes diferentes de zero, i.e., $f(x) = k, k \in K(\neq 0)$. (Para $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$)

Exemplo4: $f(x) = 6x + 3$ em $\mathbb{Z}[x]$ é fatorável como $f(x) = 3(2x + 1)$, onde os fatores são elementos não invertíveis. No entanto, em $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ este polinômio é irredutível (só possui fatoração trivial).

2) Raízes

Lema Todo polinômio de grau 1 em $K[x]$ é irredutível.
Dem.: Para um polinômio de grau 1 a única fatoração possível é um polinômio de grau 0 e outro de grau 1. No entanto, todo polinômio de grau 0 em $K[x]$ é invertível, e portanto esta fatoração será sempre trivial. ∎

Lema Considere $f(x) \in K[x]$ e $c \in K$. $f(c) = 0$ se, e somente se $f(x) = g(x)(x - c)$.
Dem.: Exercício.

Corolário Se grau$(f(x)) > 1$ e existe $c \in K$ com $f(c) = 0$ então $f(x)$ não é irredutível, ou seja, é fatorável.

Obs: A recíproca não é verdadeira, pois $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ não possui raíz em $\mathbb{R}$, mas pode ser fatorado em polinômios de grau 2. No entanto temos o

Lema Todo polinômio em $K[x]$ de grau 2 ou 3 que não possui raíz em K é irredutível.

Dem.: Para tal teríamos que $f(x) = g(x)(x - c)$, onde $g(x)$ teria grau 1 ou 2. É impossível pois neste caso "c" seria raíz. ∎

Obs: Este fato é importante porque num corpo finito ($\mathbb{Z}_p$, p primo por exemplo) podemos testar todos os elementos.

Exemplo1: $\bar{1}X^2 + \bar{3}X + \bar{4}$ em $\mathbb{Z}_5[x]$. Temos que testar $\bar{0}, \ldots, \bar{4}$.

Caso não seja raíz implica que é irredutível. Caso tenha raíz implica que é fatorável. Caso o grau do polinômio fosse 3 a conclusão seria a mesma.

Exemplo2: $\bar{2}X^4 + \bar{1}X^2 + \bar{3}X + \bar{2}$ em $\mathbb{Z}_7[x]$. Caso tenha raíz implica que é fatorável. Caso não tenha raíz implica que NADA PODEMOS AFIRMAR (com o uso deste critério !). Este é o caso para polinômios de grau igual ou maior que 4.

Exercícios:

1) Considere $f(x) \in \mathbb{R}[x]$. Se $\lambda \in \mathbb{C}$ uma raíz então seu conjugado $\bar{\lambda}$ também é raíz, ou seja, $\lambda = a + bi$, $\bar{\lambda} = a - bi, f(\lambda) = f(\bar{\lambda}) = 0$ Dica: Considere que a conjugação é um isomorfismo em $\mathbb{C}$.
2) Utilize o exercício anterior para provar que todo $f(x) \in \mathbb{R}[x]$ de grau ímpar possui pelo menos uma raíz real. Dica: As raízes complexas aparecem aos pares.
3) Utilize o teorema do valor intermediário para a função polinomial (que é sempre continua) $f(x)$ com grau ímpar e conclua o mesmo do exercício anterior.
4) Todo $f(x) \in \mathbb{R}[x]$ pode ser fatorado em polinômios de grau 1 ou 2.

3) Lema de Gauss

Este assegura que caso seja irredutível em $\mathbb{Z}[x]$ o polinômio é irredutível em $\mathbb{Q}[x]$. É claro que caso seja irredutível em $\mathbb{Q}[x]$ é irredutível em $\mathbb{Z}[x]$.

Lema Se $f(x) \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Z}[x]$ então é irredutível em $\mathbb{Q}[x]$.
Dem.: Veja em [GON] pág. 82.

4) Corpo Finito

Lema Seja p um número primo. Se $f(x) \in \mathbb{Z}[x]$ vamos definir $\bar{f}(x) \in \mathbb{Z}_p[x]$ tomando a classe de cada coeficiente de $f(x)$. Então se p não divide a_n e $\bar{f}(x)$ é irredutível sobre $\mathbb{Z}_p$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.
Dem.: Veja [GON] pág.85

5) Critério de Eiseinstein

Consultar [GON] pág.83.

6) Resumo dos Irredutíveis

$\mathbb{C}[x]$ – Somente os polinômios de grau 1, $(x - c)$, $c \in \mathbb{C}$.

$\mathbb{R}[x]$ – Os polinômios de grau 1 e os de grau 2 que possuam raízes complexas.

$\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ – Os polinômios de grau 1, e para graus maiores temos que utilizar outros critérios, como o da raíz, o de Eiseinstein etc.

$\mathbb{Z}[x]$ – Os polinômios constantes primos ($f(x) = 7, f(x) = 11$), os polinômios de grau 1 que não possuam um fator constante que possa ser retirado para fatorar ($f(x) = 9x - 3 =$

$3(3x-1)$). Para outros polinômios temos que utilizar os critérios anteriormente citados.

Exercícios:

1) Prove que se $f(x) \in K[x]$, K corpo, $\exists a \in K, f(a) = 0$ se, e somente se $f(x) = q(x)(x-a), q(x) \in K[x]$.
2) Faça os seguintes exercícios do [GON]:
   a) pág.69: 1, 4, 5, 6, 8, 11, 12, 16, 21, 22.
   b) pág.74: 2, 3, 9, 10.
   c) pág.78: 2, 6, 7.
   d) pág.81: 5, 6, 7, 8, 10.
3) Seja um domínio $D, f(x), g(x) \neq 0 \in D[x]$.
   a) Mostre que grau(f(x)*g(x)) = grau(f(x)) + grau(g(x))
   b) Dê um exemplo em $A[x]$, onde A é anel em que isto não seja verdade.
4) Prove que o anel $(\mathbb{Z}[x], +, *)$ não é um domínio de ideais principais (Dica: Tente ver o ideal gerado por x e por 2).
5) Mostre que $\mathbb{R}[x, y]$ não é domínio principal (Dica: Considere o ideal gerado por x e y).
6) Mostre que $f(x) = x^4 + x^3 + x^2 + x + 1$ não é irredutível em $\mathbb{R}[x]$.
7) Considere $f(x) = \bar{1}x^3 + \bar{1}x^2 + \bar{1}$. Mostre que $f(x)$ é irredutível em $\mathbb{Z}_2[x]$. Investigue em $\mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$.
8) Seja p um primo e $f(x) \in \mathbb{Z}_p[x]$ irredutível de grau n. Mostre que $\mathbb{Z}_p[x]/f(x)$ é corpo com p^n elementos.

IX – Extensões Algébricas

1) Introdução

Nosso objetivo aqui será gerar a partir de um corpo K, um corpo maior $K' \supset K$. Um caminho seria o processo que fazemos para passar de $\mathbb{Q}$ para $\mathbb{R}$, através de limites (ver apêndice 5). Aqui, no entanto, todas as extensões serão feitas da seguinte forma: Dado um corpo $L \supset K, \lambda \in L$ raíz de $f(x) \in K[x]$ irredutível, definimos $K[\lambda] = \{g(\lambda); g(x) \in K[x]\}$. Veremos que isto será um corpo entre L e K.

2) Conceitos Básicos

Definição: ALGÉBRICOS e TRANSCENDENTES – Dizemos que $\lambda \in L$ é algébrico sobre K se, e somente se existe $f(x) \in K[x] \setminus \{0\}$ tal que $f(\lambda) = 0$. Caso contrário dizemos que λ é transcendente (ver [GON] pág. 88).

Definição: $\text{irr}(\lambda, K)$ – Caso λ seja algébrico sobre K, $\text{irr}(\lambda, K)$ é o polinômio mônico irredutível $f(x)$ tal que λ é uma raíz.

A seguir daremos um teorema que resume toda esta história. Para ver com detalhes consulte [GON] pág.89.

Teorema Seja $\lambda \in L \supset K$. Definimos o ideal (verifique !) $I = \{f(x); f(\lambda) = 0\}$. Temos que $K[x]/I \simeq K[\lambda]$. Caso λ seja algébrico, teremos um corpo ($I = \text{irr}(\lambda, K)K[x]$). Caso seja transcendente, teremos um domínio de integridade isomorfo a $K[x]$ ($I = \{0\}$).

Dem.: Consulte [GON].

Definição: GALOISIANO – Denota-se $\text{Gal}(f, K)$. É o menor sub-corpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$. É construído da seguinte forma: Calcula-se todas as raízes $a_1, \ldots, a_n$ de $f(x)$ em $\mathbb{C}$ e $\text{Gal}(f, K) = K[a_1, a_2, \ldots, a_n]$.

Exercício: Seja $\alpha \in K$. Prove as seguintes regras de simplificação:

a) $K[\alpha\beta] = K[\beta]$

b) $K[\alpha, a_2, \ldots, a_n] = K[a_2, \ldots, a_n]$

Teorema (Elemento Primitivo) Seja $L \supset K \supset \mathbb{Q}$ tal que L seja uma extensão algébrica de K. Então, $\exists u \in L$ tal que $L = K[u]$.

Dem.: Consulte [GON] pág. 102.

Obs1: Este teorema mostra que mesmo que o galoisiano seja feito passo a passo podemos escolher um elemento de modo que baste um passo para se obter este corpo.

Obs2: Para calcular u tal que $\mathbb{Q}[u] = \mathbb{Q}[a, b]$ tome $a_1 = a$ e $a_2, \ldots, a_n$ as outras raízes de $\text{irr}(a, \mathbb{Q}), b_1 = b$ e $b_2, \ldots, b_n$ as outras raízes de $\text{irr}(b, \mathbb{Q})$. Considere os seguintes números complexos: $j \neq 1, \lambda_{ij} = \frac{a_i - a}{b - b_j} \in \mathbb{C}$. Escolha um $\lambda \in K$ tal que $\lambda \neq \lambda_{ij}$. Finalmente $u = a + \lambda b$. Um bom chute que quase sempre funciona é $u = a + b$.

3) Aplicando em $\mathbb{Q}$

Definimos todos os conceitos com um corpo K qualquer. Faremos agora uma revisão informal com $K = \mathbb{Q}$ e $L = \mathbb{R}$ ou $\mathbb{C}$.

Quando falamos que um número $\lambda \in \mathbb{R}$ é algébrico queremos dizer que ele é algébrico sobre $\mathbb{Q}$, ou seja, raíz de um polinômio em $\mathbb{Q}[x]$. caso contrário é transcendente.

Definição: GRAU – O grau de um $\lambda \in \mathbb{C}$ é definido como o grau de $f(x)$ de menor grau tal que $f(\lambda) = 0$.

Exemplo1: $\sqrt{2}$ é algébrico de grau 2, pois para $f(x) = x^2 - 1$, $f(\sqrt{2}) = 0$. Embora seja raíz de $f(x) = x^4 - 4x^2 + 4$, este não é o de menor grau.

Exemplo2: $\forall a \in \mathbb{Q}$, $f(x) = x - a$, $f(a) = 0$, ou seja, grau de a é 1. O conceito de números algébricos generaliza o de números racionais.

Exemplo3: $\sqrt{2} + \sqrt{3}$ é algébrico de grau 4.

Exemplo4: "π" e "e" são transcendentes em $\mathbb{Q}$, não são raízes de nenhum polinômio em $\mathbb{Q}[x]$. No entanto, em $\mathbb{R}[x]$ eles são algébricos: Tome $f(x) = x - \pi$, $f(x) = x - e$. A prova da transcendência de "π" e "e" exige métodos analíticos. Aos interessados remeto a livros de cálculo e análise.

Exercícios:

1) Determine o grau de:
   a) $\sqrt[4]{1 + \sqrt{2}}$
   b) $\sqrt{2} + \sqrt{8}$
   c) α raíz de $f(x) = x^8 - 4x^4 + 4$
   d) $i + 1$
   e) $i\sqrt{2}$
2) Demonstre que β é número racional se, e somente se a expansão decimal de β apresenta dízima periódica. Exemplo: $1,2174\overline{23}$ (23 repete). Entenda como dízima periódica o 0 se repetindo, $2,5 = 2,5000000\ldots$ Dica: Para volta utilize o algoritmo para expressar um número com dízima periódica como fração. Para ida mostre que o resto repete após k divisões, o que implicará que teremos k dígitos repetindo-se indefinidamente. ([BIR] pág. 97).

3) Construa um número irracional diferente de "π" e "e". Dica: Construa um número com dízima aperiódica.
4) Utilize 2) para demonstrar que $\mathbb{Q}$ é denso em $\mathbb{R}$, ou seja, dado um $a \in \mathbb{R} \setminus \mathbb{Q}$ (irracional) $\forall \varepsilon > 0\, \exists q \in \mathbb{Q}$, $|a - q| < \varepsilon$. Em outras palavras, todo número irracional pode ser aproximado por um racional tão perto quanto se queira. Dica: Trunque a expansão decimal de a e comece uma dízima periódica. Faça isto na casa decimal n tal que $10^{-n} < \varepsilon$.
5) Demonstre que todo número racional pode ser aproximado por um irracional tão perto quanto se queira. Dica: Utilize 2) e 3).

4) Dimensão

Nosso objetivo será calcular a dimensão de uma extensão algébrica qualquer através de dois teoremas que daremos a seguir. Para tal utilizaremos conceitos da álgebra linear como bases e dimensão de espaços. Em caso de dúvida consulte qualquer livro de álgebra linear.

Definição: $[V : K]$ – Significa a dimensão do espaço vetorial V sobre o corpo dos escalares K.

Teorema Seja u algébrico sobre K e grau de $\mathrm{irr}(u, K) = n$. Então $K[u]$ além de corpo é um espaço vetorial sobre K com base $1, u, u^2, \ldots, u^{n-1}$, portanto de dimensão $n = [K[u] : K]$.
Dem.: Ver [GON] pág.90 e 98.

Corolário $K[u]$ terá dimensão finita se, e somente se é algébrico sobre K. Similarmente, $K[u]$ terá dimensão infinita se, e somente se u é transcendente.

Obs: Considere $L = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2}, \ldots]$. É uma extensão algébrica de dimensão infinita. Toda extensão de dimensão finita é algébrica, mas extensões de dimensão infinita podem ser algébricas ou transcendentes. Este exemplo não contradiz o corolário pois não existe $u \in L, L = \mathbb{Q}[u]$ e u raíz de polinômio em $\mathbb{Q}[x]$.

Teorema Sejam $M \supset L \subset K$ corpos tais $[M : L]$ e $[L : K]$ são finitos. Então $[M : K] = [M : L] \cdot [L : K]$.
Dem.: Ver [GON] pág.99.

Com o primeiro teorema aprendemos a calcular a dimensão de uma extensão em que se acrescenta somente um elemento, bastando saber o grau do $\mathrm{irr}(u, K)$. Com o segundo teorema aprendemos a calcular a dimensão no caso em que acrescentamos mais de um elemento, bastando fazer um processo indutivo.

Exemplo1: O grau de $\mathbb{Q}[\sqrt[4]{2}]$ é 4, pois $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$, um polinômio de grau 4.

Exemplo2: O grau de $\mathbb{Q}[\sqrt[4]{2}, i]$ é 8, pois $\mathrm{irr}(i, \mathbb{Q}[\sqrt[4]{2}]) = x^2 + 1$, sendo portanto o grau final o produto dos graus do primeiro vezes o grau do segundo, $4 \cdot 2 = 8$.

5) Automorfismos

Nosso objetivo aqui é caracterizar todos os automorfismo de extensões algébricas de $\mathbb{Q}$ e determinar o seu número.

Lema Seja K um corpo e $\varphi \in \mathrm{Aut}(K)$. Então $A = \{x \in K; \varphi(x) = x\}$ é subcorpo de K (os elementos mantidos fixos pelo automorfismo).

Dem.: Exercício.

Exercício: Mostre que os elementos de um corpo K mantidos fixos por todos automorfismos de K formam um subcorpo. Dica: A intersecção de corpos é ainda um corpo.

Definição: CORPO PRIMO – Dado um corpo L, P é seu corpo primo caso ele seja o menor subcorpo de L. P será igual a intersecção de todos subcorpos de L.

Obs: O corpo primo de qualquer extensão de $\mathbb{Q}$ é o próprio $\mathbb{Q}$. Deste modo o corpo primo de $\mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{2}]$ etc é $\mathbb{Q}$.

Teorema Seja L um corpo e $P \subset L$ seu corpo primo. Então $\forall \varphi \in \mathrm{Aut}(L), \forall a \in P, \varphi(a) = a$.
Dem.: Seja $\varphi \in \mathrm{Aut}(L)$. Defina A como os elementos mantidos fixos pelo automorfismo φ. Pelo lema anterior, A é corpo. Como P é o subcorpo primo (a intersecção de todos os subcorpos de L) $P \subset A$, portanto $\forall a \in P, \varphi(a) = a$. ∎

Definição: $\mathrm{Aut}_K L$ – Conjunto dos automorfismos de L que mantém fixo todos os elementos de K.

Obs1: Este conjunto forma um grupo com a operação de composição de funções (prove !), o chamado grupo de automorfismos de L que mantém fixo os elementos de K.

Obs2: Como para toda extensão $L \supset \mathbb{Q}$, o corpo primo de L é $\mathbb{Q}$, $\mathrm{Aut}_{\mathbb{Q}} L = \mathrm{Aut}\, L$.

Exercícios:
1) Seja $f(x) \in \mathbb{Q}[x]$, $L = \mathrm{Gal}(f, \mathbb{Q})$, λ raíz de $f(x)$ e $\varphi \in \mathrm{Aut}\, L$. Então $\varphi(\lambda)$ é raíz de $f(x)$.
2) No exercício anterior mostre que caso $f(x)$ seja irredutível em $\mathbb{Q}[x]$ então $\mathbb{Q}[\lambda] \simeq \mathbb{Q}[\varphi(\lambda)]$. Dica: Utilize o primeiro teorema desta seção, que diz que $K[\lambda] \simeq K[x]/I$.

Teorema Todo automorfismo de $\mathbb{Q}[u]$ é da forma: $\varphi(a+bu) = a + bv$, $a, b \in \mathbb{Q}$, $\mathrm{irr}(u, \mathbb{Q}) = \mathrm{irr}(v, \mathbb{Q})$.
Dem.: $\varphi(a + bu) = \varphi(a) + \varphi(b)\varphi(u) = a + b\varphi(u)$. Como u é raíz de $\mathrm{irr}(u, \mathbb{Q}), \varphi(u) = v$ também é raíz de $\mathrm{irr}(u, \mathbb{Q})$, ou seja, $\mathrm{irr}(u, \mathbb{Q}) = \mathrm{irr}(v, \mathbb{Q})$. Obs: Sabemos que φ automorfismo, $\forall a \in \mathbb{Q}; \varphi(a) = a$. ∎

Portanto os automorfismos de corpos levam raíz em raíz, mais do que isto, a única maneira de termos automorfismos em $\mathbb{Q}[u]$ é levando u nas outras raízes de $\mathrm{irr}(u, \mathbb{Q})$. O detalhe é que nem sempre as outras raízes pertencem a $\mathbb{Q}[u]$, conforme veremos abaixo.

Exemplo1: Os automorfismos de $\mathbb{Q}[\sqrt{2}]$. $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 = \mathrm{irr}(-\sqrt{2}, \mathbb{Q})$. Portanto temos φ levando $\sqrt{2}$ em $\sqrt{2}$ e outro automorfismo levando $\sqrt{2}$ em $-\sqrt{2}$, ou seja, $|\mathrm{Aut}\, \mathbb{Q}[\sqrt{2}]| = 2$.

Exemplo2: Os automorfismos de $\mathbb{Q}[\sqrt[4]{3}]$. $\mathrm{irr}(\sqrt[4]{3}, \mathbb{Q}) = x^4 - 3$. Temos quatro raízes: $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $i\sqrt[4]{3}$, $-i\sqrt[4]{3}$. No entanto, somente as duas primeiras raízes pertencem a $\mathbb{Q}[\sqrt[4]{3}]$, e portanto $|\mathrm{Aut}\, \mathbb{Q}[\sqrt[4]{3}]| = 2$.

Exemplo3: Os automorfismo de $\mathbb{Q}[\sqrt[4]{3}, i]$. Temos que $\mathrm{irr}(\sqrt[4]{3}, \mathbb{Q}) = x^4 - 3$, $\mathrm{irr}(i, \mathbb{Q}[\sqrt[4]{3}]) = x^2 + 1$. As quatro raízes de $x^4 - 3$ pertencem ao corpo, bem como as duas raízes i e $-i$. Portanto temos quatro opções para $\sqrt[4]{3}$ e duas para i, o que dá: $|\mathrm{Aut}\, \mathbb{Q}[\sqrt[4]{3}, i]| = 4 \cdot 2 = 8$.

Daremos agora a "receita de bolo" para se encontrar o número de automorfismos de extensões L de $\mathbb{Q}$:

1. Escrever $L = \mathbb{Q}[u_1, u_2, \ldots, u_n]$.

2. Denotando $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}[u_1]$, $K_2 = \mathbb{Q}[u_1, u_2]$,..., $K_n = L$, considere $f_1(x) = \text{irr}(u_1, K_0)$, $f_2(x) = \text{irr}(u_2, K_1)$,..., $f_n(x) = \text{irr}(u_n, K_{n-1})$.

3. Para cada $f_n(x)$ considere o número de raízes distintas que pertencem ao corpo L.

4. $|\text{Aut}\, L|$ é o produto do número de raízes distintas (pertencentes ao corpo L) de cada $f_n(x)$.

Obs: Deve-se evitar redundâncias na representação de $L = \mathbb{Q}[u_1, u_2, \ldots, u_n]$, de modo que fique na forma mínima. Por exemplo, $\mathbb{Q}[\sqrt{2}, i, -i\sqrt{2}] = \mathbb{Q}[\sqrt{2}, i]$.

Teorema $|\text{Aut}\, L| = |L : \mathbb{Q}|$ se, e somente se L é uma extensão galoisiana.

Dem.: Ver [GON].

Obs: Pelo teorema anterior o número de automorfismos é igual ao grau da extensão se, e só se a extensão é galoisiana. De modo geral o número de automorfismo é menor ou igual ao grau da extensão.

X – Introdução à Teoria de Galois

A aplicação mais comum desta teoria é para se verificar a solubilidade por meio de radicais de raízes de polinômios, isto é, a existência de fórmulas envolvendo operações aritméticas básicas (soma, subtração, multiplicação e divisão) e radiciações (raízes quadradas, cúbicas etc.) para determinar raízes de polinômios. Podemos demonstrar que existem polinômios de grau maior ou igual a 5 para os quais não existe uma expressão radical fechada para calcular suas raízes.

O conceito mais importante a ser entendido inicialmente é como um corpo pode gerar um grupo e como um grupo pode gerar um corpo. Nós vimos na parte de extensões como um corpo $K \subset L$ gera o grupo dos automorfismos de L que mantém fixo K, ou seja, $Aut_K L$. Dado um corpo intermediário $M, K \subset M \subset L$ podemos gerar o grupo $\text{Aut}_M L$, que será um subgrupo de $\text{Aut}_K L$. Ele será um subgrupo pois aumentando o número de elementos a serem mantidos fixos diminuem o número de automorfismos.

Similarmente dado um subgrupo G de $\text{Aut}_K L$ temos o corpo fixo deste grupo, ou seja, o corpo
$M = \{u \in L; \varphi(u) = u \ \forall \varphi \in G\}$, que estará entre K e L $(K \subset M \subset L)$.

No caso da teoria de Galois devemos considerar um corpo K e uma extensão algébrica galoisiana L , ou seja, $L = \text{Gal}(f, K)$ para algum $f(x) \in K[x]$. Agora queremos encontrar corpos intermediários M tais que $L \supset M \supset K$.

Teorema (Teorema fundamental de Galois) A cada subcorpo de L que seja uma extensão galoisiana de K corresponde um subgrupo normal de $\text{Aut}_K L$. Similarmente a cada subgrupo normal corresponde uma extensão galoisiana.

Dem.: Ver [FRA].

Definição: GRUPO SOLÚVEL – Um grupo é solúvel se existe uma seqüência de subgrupos, cada um subgrupo normal do anterior, e os grupos quocientes sucessivos são abelianos.

A relação com a solubilidade por meio de radicais foi dada por Evariste Galois:

Teorema Um polinômio é solúvel por meio de radicais se, e só se, o grupo $\text{Aut}_K L$, onde $L = \text{Gal}(f, K)$, é solúvel.

Dem.: Ver [FRA].

Para demonstrar a existência de um polinômio de grau 5 cujas raízes não podem ser expressas por meio de radicais o roteiro é:

1. Estudar o subgrupo do S_5 (grupo das permutações de um conjunto com 5 elementos) formado pelas permutações pares, denotado por A_5. O A_5 não é abeliano e não possui subgrupo normal não-trivial. Isto implica que S_5 não é solúvel.

2. Estudar um polinômio de grau 5 cujo grupo de automorfismos é o S_5.

3. Portanto não existe fórmula por meio de radicais para determinar as raízes deste polinômio.

Obs1: Prova-se que, para $n > 4$, A_n (subgrupo das permutações pares de S_n) é simples, i.e., não possui subgrupo normal diferente dos triviais (zero e o próprio). Isto implica que S_n não é solúvel para $n > 4$. Ver qualquer livro de álgebra (por exemplo [HER]).

Obs2: Pode-se exibir um polinômio de grau n para qualquer n tal que o grupo de automorfismos é o S_n. Portanto, utilizando-se a observação anterior, para $n > 4$ existe polinômio de grau n que não é solúvel por meio de radicais. Dai decorre a impossibilidade de fórmulas para polinômios com grau maior, ou igual a 5.

Obs3: Os grupos simples têm uma importância similar aos números primos. Os grupos simples não possuem subgrupo normal diferente dos triviais e os primos não possuem divisor diferente dos triviais (ele próprio e a unidade).

XI – Apêndices

1) Como Demonstrar

Reconhecendo ser as demonstrações a parte mais difícil do aprendizado de Matemática, gostaria de explicar como acho correto proceder. O mais importante é que a formalização seja o último passo deste processo.

1.1) Delineamento

Em primeiro lugar devemos ter claro o que é a hipótese e o que é a conclusão a que se deseja chegar. Para não haver problemas nesta parte, devemos escrever claramente o que desejamos provar com uma interrogação ao lado. Ao começarmos a demonstração devemos reescrever as hipóteses.

Deve-se prestar atenção se o problema é do tipo: A $\Longrightarrow$ B ou B $\Longrightarrow$ A ou A $\Longleftrightarrow$ B. Neste último caso devemos separar a demonstração em duas partes: A ida (A $\Longrightarrow$ B) e a volta (B $\Longrightarrow$ A).

1.2) Pensar intuitivamente

Agora devemos procurar entender o que está sendo pedido, tentando exemplos conhecidos, casos particulares, etc. Devemos procurar desenhar, discutir com um colega, evitando nesta fase uma formalização precipitada. Através de alguns exemplos verificamos a validade ou não de nosso raciocínio. Quando o seu professor faz demonstrações diretamente em linguagem formalizada pode ter certeza: quando ele estava aprendendo fazia o mesmo. É uma questão de nível, para ele tudo isto são trivialidades, mas para os problemas que ele tenta resolver como um pesquisador em Matemática, o processo de abordagem é o mesmo, o da intuição.

1.3) Formalizar

Proceder a formalização passo a passo, eventualmente pulando alguns detalhes. Com isto quero dizer que se ao longo de uma demonstração necessitar de um fato não demonstrado, assuma que vale, termine a demonstração, a seguir demonstrando o que faltou. Para quem sabe computação, é como se o fato não demonstrado fosse uma subrotina do programa principal.

2) Teorema Fundamental da Álgebra

Este teorema afirma que todo polinômio em $\mathbb{C}[x]$ apresenta raízes em $\mathbb{C}$. O interessante é que não existe prova algébrica deste teorema, sendo necessário se recorrer a análise complexa (ou topologia algébrica) para demonstrá-lo.

3) Solução por Radical

Uma expressão radical é uma expressão que envolve somente operações simples, como multiplicações, divisões, somas, subtrações e radiciações.

Durante muito tempo procurou-se por uma expressão radical que fosse a fórmula para calcular as raízes de um polinômio geral. Ao longo da História foram surgindo expressões radicais para resolver os polinômios de grau 2, 3 e 4. Procurou-se em vão pela expressão de grau 5 até que Abel demonstrou que não existia expressão radical para polinômios de grau 5.

Evariste Galois deu a resposta definitiva com um critério geral para determinar se uma equação polinomial dada possui solução por expressão radical ou não (ver a parte X – Introdução à Teoria de Galois). Deste critério resulta que existem polinômios de grau maior ou igual a 5 para os quais não existe uma expressão radical para suas raízes.

Nestes casos, apesar de termos raízes asseguradas pelo teorema fundamental da Álgebra, teremos que utilizar métodos numéricos para obter as raízes.

4) Corpo de Frações de um Domínio

Aqui demonstraremos que todo domínio de integridade pode ser estendido de forma que se torne um corpo, i.e., todo elemento tenha inverso multiplicativo.

O processo de construção deste corpo é feito em completa analogia com a construção de $\mathbb{Q}$ a partir $\mathbb{Z}$:

1. Definiremos um novo conjunto K, gerado por D de uma forma adequada.

2. Definiremos novas operações de soma e produto neste conjunto de forma que K vire um corpo.

3. Colocaremos o domínio D dentro do novo corpo K, de modo que de alguma forma $D \subset K$, da mesma forma que podemos colocar $\mathbb{Z} \subset \mathbb{Q}$.

4.1) Definindo o novo conjunto

Considere $K' = D \times D^*$, onde $D^* = D \setminus \{0\}$. K' será formado por pares ordenados (a, b), onde $a \in D$ e $b \in D^*$. No entanto vamos denotar (a, b) por a/b.

Agora defina a seguinte relação de equivalência em K': $(a/b) \sim (c/d)$ se, e somente se $a * d = b * c$ (foi passado como exercício verificar que é relação de equivalência !).

Finalmente $K = K'/\sim$, ou seja, cada elemento de K é uma classe de equivalência em K'.

Exemplo: Em $\mathbb{Z} \times \mathbb{Z}^*$, $(6/9) = (2/3)$, pois $2 * 9 = 3 * 6$.

4.2) Definindo novas operações

Em K, definiremos $a/b *' c/d = (a*c)/(b*d)$, e para $a/b +' c/d = (a*d+b*c)/(b*d)$. Resta verificar se estas operações estão bem definidas, ou seja, tomando $x_1, x_2, y_1, y_2 \in K'$, com $\bar{x}_1 = \bar{x}_2$ e $\bar{y}_1 = \bar{y}_2$, verificar se $\bar{x}_1 +' \bar{y}_1 = \bar{x}_2 +' \bar{y}_2$ (mesmo para o produto). Não procederemos com esta verificação, mas o leitor poderá recorrer a [GAR], pág.38.

Obs: Quando falamos que $\bar{x}_1 = \bar{x}_2$ queremos dizer que tomamos dois representantes da mesma classe de equivalência, ou seja, $x_1 = a/b, x_2 = c/d$, com $a * d = b * c$. Em $\mathbb{Z}$ poderíamos tomar $x_1 = 9/6$ e $x_2 = 18/12$.

Teríamos que verificar agora se $(K, +', *')$ é de fato um corpo, quem é o zero, o elemento neutro da multiplicação, etc. Além disto teríamos que colocar D dentro de K. Todo este trabalho fica por conta do leitor, que em caso de dúvida poderá recorrer à referência supra citada.

5) Construção dos Conjuntos Numéricos

5.1) Construção de $\mathbb{N}$

Não procederemos a esta construção básica, que consiste em axiomatizar os inteiros $\mathbb{N}$ com os axiomas de Peano. Destes decorrem todas as propriedades de $\mathbb{N}$. Para tal consulte [HAL] pág. 46.

O mais importante na construção de Peano é a função sucessor, que a cada elemento de $\mathbb{N}$ associa o próximo. Seria como somar "mais um".

Define-se a soma por indução com a função sucessor, e o produto através da soma. Define-se também uma relação de ordem.

5.2) Construção de $\mathbb{Z}$

Dada a existência de $\mathbb{N}$ podemos construir $\mathbb{Z}$ do seguinte modo:

1. Defina o conjunto $Z' = \mathbb{N} \times \mathbb{N}$.

2. Defina em Z' a relação de equivalência $(a, b) \sim (c, d)$ se, e somente se $a - b = c - d$.

3. Defina $\mathbb{Z} = Z'/\sim$.

4. Defina em $\mathbb{Z}$ a soma e o produto através da soma e produto em $\mathbb{N}$:

$(a,b)+'(c,d) = (a+c, b+d)$ e $(a,b)*'(c,d) = (a*c+b*d, b*c+a*d)$

5. Verifique se as operações estão bem definidas.

6. Veja que agora todo elemento terá inverso aditivo.

7. Teremos todas as propriedades necessárias: Comutatividade, associatividade, distributividade etc.

8. Desta forma $\mathbb{Z}$ será um domínio de integridade.

5.3) Construção de $\mathbb{Q}$

Foi feita no apêndice anterior, através do corpo de frações do domínio $\mathbb{Z}$.

5.4) Construção de $\mathbb{R}$

Para esta construção necessitaremos de algo mais do que conceitos puramente algébricos. A passagem de $\mathbb{Q}$ para $\mathbb{R}$ necessita de conceitos analíticos.

A diferença destes corpos será que $\mathbb{R}$ é um corpo completo, ou seja, toda seqüência de Cauchy converge. Na realidade a única razão para uma seqüência de Cauchy não convergir é a existência de um "buraco" no espaço.

Obs: Uma seqüência de Cauchy é uma seqüência em que os termos sucessivos estão cada vez mais próximos. Para uma definição precisa veja [LIM] pág.98.

Exemplo: A seqüência $(1, 1.4, 1.41, 1.414, \ldots)$ é seqüência de Cauchy convergindo para $\sqrt{2}$. Em $\mathbb{Q}$ esta seqüência não é convergente pois $\mathbb{Q}$ apresenta "lacunas".

1. Definimos o conjunto R' das seqüências de Cauchy de números racionais, ou seja, $(a_n), a_n \in \mathbb{Q}$, tais que a seqüência seja de Cauchy.

2. Definimos a relação de equivalência, $(a_n) \sim (b_n)$ se, e somente se $\lim_{n\longrightarrow\infty}(a_n - b_n) = 0$

3. Agora o conjunto $\mathbb{R}$ será $R'/\sim$.

4. Definimos a soma e o produto em $\mathbb{R}$ como o limite da soma dos termos da seqüência em $\mathbb{Q}$, ou seja, $\overline{(a_n)} +' \overline{(b_n)} = \overline{(a_n + b_n)}$, analogamente para o produto.

5. Agora resta verificar se estas operações estão bem definidas, se temos de fato um corpo etc. Poderemos também definir uma relação de ordem em $\mathbb{R}$ a partir da relação de ordem em $\mathbb{Q}$, que por sua vez é definida a partir da relação de ordem de $\mathbb{N}$.

Obs1: Podemos axiomatizar $\mathbb{R}$ através da propriedade do supremo, ou seja, que todo conjunto limitado de $\mathbb{R}$ possui supremo.

Obs2: Outra maneira clássica de construir $\mathbb{R}$ é através de cortes de Dedekind.

5.5) Construção de $\mathbb{C}$

Esta construção já deve ter sido feita como um exercício. Ela envolve somente conceitos algébricos. No entanto a caracterização principal de $\mathbb{C}$, o fato de ser um corpo algebricamente fechado, conforme já foi visto, envolve conceitos não algébricos.

1. Dividir o domínio $\mathbb{R}[x]$ de polinômios pelo ideal maximal gerado pelo polinômio irredutível x^2+1, ou seja, o conjunto $\mathbb{C}$ será $\mathbb{R}[x]/I$, onde $I = (x^2+1)\mathbb{R}[x]$.

2. Define-se as operações de soma e produto da forma usual, sendo que neste caso é impossível definir-se uma relação de ordem como nos anteriores.

Obs: Outra maneira de definir $\mathbb{C}$ é definir no conjunto de pares ordenados $(a,b) \in \mathbb{R}\times\mathbb{R}$ as operações de soma e produto destes pares de forma apropriada. Depois introduzir a notação $a+bi$.

6) Outros Corpos

Seguindo o caminho de obter $\mathbb{C}$ a partir de $\mathbb{R}$, um corpo de dimensão 2 sobre $\mathbb{R}$, podemos ser tentados a obter corpos que contenham $\mathbb{R}$, porém de dimensão maior que 2. Podemos provar que isto é impossível para dimensão 3 (ver [FEL] pág.3).

Hamilton conseguiu, em 1843, uma generalização dos números complexos: Os Quatérnios. Eles são um corpo de dimensão 4 sobre os reais onde a multiplicação não é comutativa.

Logo após Hamilton, Cayley obteve, não exigindo comutatividade nem associatividade, os Bi-Quatérnios, corpo de dimensão 8 sobre os Reais.

Ainda houveram muitas tentativas frustradas de se obter corpos com outras dimensões sobre os reais. Em 1877 Frobenius provou que exigindo-se associatividade os únicos corpos são: $\mathbb{R}$, $\mathbb{C}$ e Quatérnios. Restou o problema para as não associativas, resolvidas em 1957 por Bott e Milnor e Kervaire : $\mathbb{R}, \mathbb{C}$, Quatérnios e Bi-Quatérnios.

Obs: Este tópico do apêndice está inteiramente baseado em [FEL].

XII – Bibliografia

[BIR] Birkhoff, Garrett; MacLane, Saunders; – *Álgebra Moderna Básica* – Guanabara Dois, 1980.

[CAR] Caraça, Bento de Jesus – *Conceitos Fundamentais da Matemática* – Lisboa, 1958

[FEL] Felzenszwalb, Bernardo – *Álgebras de Dimensão Finitas* – IMPA – 12º – Colóquio – 1979

[FRA] Fraleigh, John – *A First Course in Abstract Algebra* – Addison-Wesley

[GAR] Garcia, Arnaldo – *Álgebra: um curso de introdução* – IMPA

[GON] Gonçalves, Adilson – *Introdução à Álgebra* – IMPA, 1979.

[HAL1] Halmos, Paul – *Teoria Ingênua dos Conjuntos* – D. Van Nostrand Company

[HAL2] Halmos, Paul – *Espaços Vetoriais de Dimensão Finita* – D. Van Nostrand Company

[HER] Hernstein, I. – *Topics in Algebra* – Blaisdell Book Co.

[LIM] Lima, Elon Lages – *Curso de Análise Vol. I* – IMPA, 1989.

[NAC] Nachbin, Leopoldo – *Introdução à Álgebra* – McGraw-Hill