Grupos e Corpos

Prof. Lucas Calixto

Aula 8 - Um resumo sobre anéis e corpos

Um anel R e um conjunto munido de duas funções (soma $+$ e produto $\cdot$):

$$+ : R \times R \to R, (a, b) \mapsto a + b, \quad \cdot : R \times R \to R, (a, b) \mapsto ab$$

tais que

1. $(R, +)$ é grupo abeliano (como usual, denotaremos por 0 o elemento identidade com respeito a soma $+$)
2. $(ab)c = a(bc)$, $\forall a, b, c \in R$
3. $a(b + c) = ab + ac$, $\forall a, b, c \in R$
4. Se $ab = ba$, $\forall a, b \in R$, dizemos que R é anel comutativo
5. Se $\exists\ 1 \in R$ tal que $1a = a1 = a$, $\forall a \in R$, dizemos que R é anel com identidade. O elemento 1 e chamado de elemento identidade com respeito ao produto $\cdot$

Nesse curso só vamos nos interessar por anéis comutativo com identidade, portanto durante nossas aulas

anel = anel comutativo com identidade

Um elemento $a \in R$ é invertível se $\exists\ a^{-1} \in R$ tal que $aa^{-1} = 1$. Se todo $a \in R \setminus \{0\}$ é invertível, dizemos que R é um corpo. R corpo $\Rightarrow (R, +)$ e $(R \setminus \{0\}, \cdot)$ são grupos abelianos

Definimos a característica do anel R por $\text{car}(R) = |1|$ se $|1| < \infty$, e $\text{car}(R) = 0$ se $|1| = \infty$ (aqui, a ordem $|1|$ é tomada com respeito a soma de R)

Exercício: Prove que os elementos $0, 1 \in R$ são únicos, e, quando existe a^{-1} também é único

Exemplo: Os principais exemplos de anéis são $\mathbb{Z}$, $\mathbb{Z}_n$ e $\mathbb{F}[x]$, onde $\mathbb{F}$ é corpo

Exemplo: Os principais exemplos de corpos são $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$

$S \subset R$ é um subanel se S for um anel com as mesmas operações de R

$I \subset R$ é um ideal de R se valem:

- $(I, +) \leq (R, +)$ (ou seja, $\forall\ a, b \in I \Rightarrow a - b \in I$)
- $r \in R,\ a \in I \Rightarrow ra \in I$

Se $a \in R$, então $(a) = Ra = \{ra \mid r \in R\}$ é o menor ideal de R que contém a. Dizemos que a gera (a). Os ideais da forma (a) são chamados de ideais principais

Note: Todo ideal próprio de $\mathbb{Z}$ é da forma $(n) = n\mathbb{Z}$ para algum $n \in \mathbb{Z}$

Exercício: Seja $I \subset R$ um ideal. Mostre que $I \neq R \Leftrightarrow \nexists\ a \in I$ invertível

Homomorfismos e quocientes

Um homomorfismo de anéis $\varphi : R \to S$ é uma função tal que, $\forall a, b \in R$:

- $\varphi(a+b) = \varphi(a) + \varphi(b) \Rightarrow$ φ é homomorfismo dos grupos abelianos $(R, +)$ e $(S, +)$
- $\varphi(ab) = \varphi(a)\varphi(b)$

Se $I \subset R$ é ideal $\Rightarrow R/I = \{r + I \mid r \in R\}$ é anel:

$$(a+I) + (b+I) = (a+b) + I, \quad (a+I)(b+I) = ab + I$$

Como em grupos, $\phi : R \to R/I$, $\varphi(a) = a + I$ é um homomorfismo de aneis (canônico)

Exercício: $\mathbb{Z}/(n) = \{a + (n) \mid a \in Z\} = \{0 + (n), 1 + (n), \ldots, n - 1 + (n)\}$ (por divisão de Euclides)

Um ideal próprio $I \subset R$ é maximal se I é maximal em $\{J \subsetneq R \mid J \text{ é ideal de } R\}$

Proposição: $I \subset R$ é maximal $\Leftrightarrow R/I$ é corpo

Exemplo: $(p) \subset \mathbb{Z}$ é maximal $\Leftrightarrow p$ é primo. Logo, $\mathbb{Z}/(p)$ é corpo $\Leftrightarrow p$ é primo

Um isomorfismo de aneis é um homomorfismo de aneis que é bijetor

Os teoremas de isomorfismo que existem para grupos também valem para anéis: trocando subgrupos normais por ideais, e subgrupos por subaneis:

1ºTI: Se $\phi : R \to S$ é homomorfismo de anéis, então $\ker \phi$ é um ideal de R e $R/\ker \phi \cong \phi(R)$

2ºTI: Se $S \subset R$ é subanel, e $I \subset R$ é um ideal, então $I \cap S$ é um ideal de S e

$$S/(I \cap S) \cong (I + S)/I$$

3ºTI: Sejam $I \subset J$ ideais de R, então

$$R/J \cong \frac{R/I}{J/I}$$

TC: Se I é ideal de R, então existe uma bijeção

$$\{S \text{ subanel de } R \mid I \subset S\} \leftrightarrow \{\bar{S} \text{ subanel de } R/I\}$$

Essa bijeção continua valida trocando a palavra subanel por ideal nos conjuntos

Pre-requisitos de Fundamentos de Álgebra - Cap. 17

- polinomio sobre um corpo
- grau de um polinomio
- polinomio monico
- divisibilidade de polinomios
- mdc entre polinomios
- polinomios coprimos
- algoritmo de Euclides para polinomios
- polinomios irredutíveis
- caracterização dos polinomios irredutíveis de $\mathbb{R}[x]$ e $\mathbb{C}[x]$
- o critério de Eisenstein

Dado um polinomio $f(x) \in \mathbb{F}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0$$

- o coeficiente lider de $f(x)$ é a_n. Escrevemos $cl(f(x)) = a_n$
- o grau de $f(x)$ é n. Escrevemos $\text{gr}(f(x)) = n$
- Se $a_n = 1$, dizemos que $f(x)$ é monico
- $\text{gr}(f(x) + g(x)) \leq \max\{\text{gr}(f(x)), \text{gr}(g(x))\}$
- $\text{gr}(f(x)g(x)) = \text{gr}(f(x)) + \text{gr}(g(x))$
- Se $f(x), g(x) \in \mathbb{F}[x]$, então existem únicos $q(x), r(x) \in \mathbb{F}[x]$ tais que

$$f(x) = g(x)q(x) + r(x),$$

onde $r(x) = 0$, ou $r(x) \neq 0$ e $\text{gr}(r(x)) < \text{gr}(g(x))$. Se $r(x) = 0$, dizemos que $g(x)$ divide $f(x)$. Escrevemos $g(x) \mid f(x)$

- $f(x) \in \mathbb{F}[x]$ é divisível por $x - a \Leftrightarrow a$ é uma raíz de $f(x)$ (ou seja, $f(a) = 0$)

• o $mdc(f(x), g(x))$ é o único polinomio monico $d(x)$ que divide ambos $f(x)$ e $g(x)$ e que é divisível por qualquer outro polinomio $q(x)$ que divida ambos $f(x)$ e $g(x)$

• se $mdc(f(x), g(x)) = 1$, dizemos que $f(x)$ e $g(x)$ são comprimos

• $f(x) \in \mathbb{F}[x]$ é redutível se $f(x) = g(x)q(x)$ com $\text{gr}(g(x)), \text{gr}(q(x)) > 0$. Dizemos que $f(x)$ é irredutível, se não for redutível

• $f(x) \in \mathbb{C}[x]$ é irredutível $\Leftrightarrow \text{gr}(f(x)) = 1$

• $f(x) \in \mathbb{R}[x]$ é irredutível $\Leftrightarrow \text{gr}(f(x)) = 1$, ou $\text{gr}(f(x)) = 2$ e $f(x)$ não admite raiz em $\mathbb{R}$

Lema de Gauss: Seja $f(x) \in \mathbb{Z}[x]$ monico. Então $f(x)$ é redutível em $\mathbb{Z}[x] \Leftrightarrow f(x)$ é redutível em $\mathbb{Q}[x]$

Critério de Eisenstein: Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Se existe um primo $p \in \mathbb{Z}$ tal que: $p \mid a_i$ para $i = 0, \ldots, n-1$, mas $p \nmid a_n$ e $p^2 \nmid a_0$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$

Considere $f(x) \in \mathbb{F}[x]$ tal que $\text{gr}(f(x)) = k$

Pelo algoritmo de Euclides, se $g(x) \in \mathbb{F}[x]$ então

$$g(x) = f(x)q(x) + r(x), \quad \text{onde } r(x) = 0, \text{ ou } \text{gr}(r(x)) < k$$

Logo,

- $\overline{g(x)} = \overline{r(x)}$ como elementos de $\mathbb{F}[x]/(f(x))$
- $\mathbb{F}[x]/(f(x)) = \{a_0 + a_1\bar{x} + \cdots + a_{k-1}\bar{x}^{k-1} \mid a_i \in \mathbb{F}\} \Rightarrow \dim_{\mathbb{F}} (\mathbb{F}[x]/(f(x))) = k$

Proposição: Se I é ideal de $\mathbb{F}[x]$, então existe único polinômio mônico $f(x) \in \mathbb{F}[x]$ tal que $I = (f(x))$. Além disso, as afirmações que seguem são equivalentes:

1. $f(x)$ é irredutível
2. I é ideal maximal
3. $F[x]/I$ é corpo (ótima ferramenta para construir corpos)

Prova: Seja $f(x) \in I$ um polinomio de grau mínimo em I

Suponha que $f(x)$ é mônico (caso não fosse, tome $cl(f(x))^{-1}f(x)$ no lugar de $f(x)$)

$(f(x)) \subset I$ é óbvio. Por outro lado, se $g(x) \in I$, então

$$g(x) = f(x)q(x) + r(x), \quad \text{onde } r(x) = 0, \text{ ou } \operatorname{gr}(r(x)) < \operatorname{gr}(f(x))$$

$r(x) = g(x) - f(x)q(x) \in I \Rightarrow r(x) = 0$ pela minimalidade do grau de $f(x)$

$\Rightarrow g(x) \in (f(x)) \Rightarrow I = (f(x))$

- Note que $(g(x)) \subsetneq (q(x)) \Leftrightarrow g(x) = t(x)q(x)$, onde $\operatorname{gr}(t(x)) > 0$

(1) $\Leftrightarrow$ (2): pela primeira parte, $(f(x))$ não é maximal $\Leftrightarrow f(x) = g(x)q(x)$ com $\operatorname{gr}(g(x)), \operatorname{gr}(q(x)) > 0$ (que é a definição de $f(x)$ ser redutível)

(2) $\Leftrightarrow$ (3): segue de exercício anterior

Exemplo: $p(x) = x^2 + 1 \in \mathbb{R}[x]$ é irredutível (pq?). Logo

$$\mathbb{F} = \mathbb{R}[x]/(p(x)) = \{a + b\bar{x} \mid a, b \in \mathbb{R}\}$$

é corpo. Além disso, $\overline{p(x)} = \bar{0} \Rightarrow \bar{x}^2 = -1$ em $\mathbb{F}$

Agora é fácil ver que $\mathbb{F} \cong \mathbb{C}$, onde o isomorfismo envia $a + b\bar{x}$ em $a + bi$

Corpo de frações

Um elemento $a \in R \setminus \{0\}$ é um divisor de zero se existe $b \in R \setminus \{0\}$ para o qual $ab = 0$

Um anel D que não tem divisores de zero é chamado um domínio

Exemplo: $\mathbb{Z}$, $\mathbb{F}[x]$ são domínios

Exemplo: $\mathbb{Z}_{pq}$ $(p, q > 1)$ não é domínio

Exemplo: Todo corpo é um domínio

Pense em $a/b \in \mathbb{Q}$ como $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Sabemos que $a/b = c/d \Leftrightarrow ad = bc$, ou seja

$$(a, b) = (c, d) \Leftrightarrow ad = bc$$

Dado um domínio D, podemos construir um corpo Q a partir de D:

- Tome $S = \{(a, b) \in D \times D \mid a, b \in D \text{ e } b \neq 0\}$
- Mostre que $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ define uma relação de equivalência em S

Denote a classe de equivalência de (a, b) por a/b

Considere o conjunto de tais classes de equivalência $Q = \{a/b \mid a, b \in D \text{ e } b \neq 0\}$

Em Q, defina $+$ e $\cdot$ da seguinte forma (imitando $\mathbb{Q}$):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{e} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Exercício: Verifique que $(Q, +, \cdot)$ é um corpo

Q é chamado de corpo de frações do domínio D

• $\iota : D \to Q$, $\iota(a) = a/1$ é um homomorfismo injetor de aneis (mergulho). Logo, $D \cong \iota(D) = \{a/1 \mid a \in D\}$ e por isso pensamos em D como subanel de Q

• Q é o menor corpo que contem D no seguinte sentido: se $\mathbb{F}$ é corpo que contem D, então existe mergulho de Q em $\mathbb{F}$. De fato, mostre que

$$\varphi : Q \to \mathbb{F}, \quad \varphi(a/b) = ab^{-1}$$

é mergulho

Exemplo: $\mathbb{F}[x_1, \ldots, x_n]$ é domínio e o seu corpo de frações é

$$\mathbb{F}(x_1, \ldots, x_n) = \{f(x_1, \ldots, x_n)/q(x_1, \ldots, x_n) \mid q(x_1, \ldots, x_n) \neq 0\}$$

Lista de exercício

Cap. 17 : 2 - d,e, 3, 8, 12, 13, 14, 20, 24, 26

Cap. 18 : 8 (fiquem a vontade para fazer qualquer outro exercício)