MAT0364\MAT6643 – Teoria de Galois

Contato: fyyasumura@ime.usp.br

Seg: 8:00 - 10:00
Qua: 10:00 - 12:00

Referência:
N. Jacobson, Basic Algebra I.

Provas: P1: 2 de junho
P2: 21 de julho

Média final: $MF = \frac{P1 + P2}{2}$,

Aprovado se $MF \geq 5$.

Formato das provas:

- início no horário de aula
- 48 horas + ε para entregar

Prova:

- 1 ex. de def. e enunciado de Teorema
- 3 ou 4 exercícios sorteado das listas,
- 1 exercício "novo" (escolher entre 3 exercícios).

Intervalos: 5 min. (± metade)

→ Eq. de grau 2: babilônios, 1600 A.C.

→ Pol. de grau 3 e 4: Cardano (1545):
- Tartaglia (Fontana): 1535,
- Ferrari: 1545

→ 1770-1771: Lagrange: unificou os métodos p/ pols. de grau ≤ 4

→ Abel, 1824: impossível resolver uma eq. de grau 5 via radicais.

→ Galois (1811 - 1832).

→ Pol. de grau 2: $x^2 + ax + b = (x - \alpha_1)(x - \alpha_2)$

$$\begin{cases} a = -(\alpha_1 + \alpha_2) \\ b = \alpha_1 \alpha_2 \end{cases}$$

$(\alpha_1 - \alpha_2)^2$ é invariante por $\alpha_1 \leftrightarrow \alpha_2$.

$\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_1$ $\quad (\alpha_1 - \alpha_2)^2$

$$(\alpha_1-\alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2$$

$$= a^2 - 4b$$

$$\begin{cases} \alpha_1 - \alpha_2 = \sqrt{a^2-4b} \\ \alpha_1 + \alpha_2 = -a \end{cases}$$

Eq. de grau 3: $X^3 + aX^2 + bX + c$.

$\alpha_1, \alpha_2, \alpha_3$ são as raízes.

$\omega^3 = 1$, $\omega \neq 1$.

$1 + \omega + \omega^2 = 0$

$1 + \omega + \omega^2 \left(\frac{1-\omega}{1-\omega}\right) = \frac{1-\omega^3}{1-\omega} = 0$

$$u = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3$$

$$v = (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3$$

→ $u+v$ e uv são invariantes pela ação de S_3.

$$\begin{cases} u+v = \dots = 2a^3 - 6c + 9ab \\ uv = \dots = (a^2-3c)^3 \end{cases}$$

⇒ Sabe quem é u e v

$$\begin{cases} -a = \alpha_1 + \alpha_2 + \alpha_3 \\ \sqrt[3]{u} = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ \sqrt[3]{v} = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \end{cases}$$

Revisão

Definição. Um anel é uma tripla $(A, +, \cdot)$, em que $+, \cdot : A \times A \to A$ satisfazendo:

(i) $(A, +)$ é um grupo abeliano,

(ii) $(a+b)\cdot c = a\cdot c + b\cdot c$, $c\cdot(a+b) = c\cdot a + c\cdot b$, $\forall a, b, c \in A$,

(iii) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$, $\forall a, b, c \in A$.

(iv) dizemos que A admite unidade se existe $1 \in A$ tal que $a\cdot 1 = 1\cdot a = a$, $\forall a \in A$,

(v) dizemos que A é comutativo se $a\cdot b = b\cdot a$, $\forall a, b \in A$.

(vi) dizemos que A é domínio (ou domínio de integridade) se $a\cdot b = 0$, ~~$\forall b \in A$~~ p/ algum $b \neq 0$ $\Rightarrow a = 0$.

Para nós, anel significa: anel comutativo com unidade.

Def. Seja A anel. Um subconjunto $S \subseteq A$ é um subanel se $a-b, ab \in S$, $\forall a, b \in S$.

Para nós: subanel entende-se também que $1_A \in S$.

Def. Um corpo F é um anel (comutativo com 1) tal que, $\forall a \in F \setminus \{0\}$, existe b satisfazendo $ab = 1$. Denota-se $a^{-1} := b$.

Observações.

(i) Todo corpo é domínio.

(ii) Todo domínio pode ser imerso num corpo (seu corpo de frações).

Def. Um subconjunto $I \subseteq A$ é ideal se:

(i) $x - y \in I$, $\forall x, y \in I$,

(ii) $ax \in I$, $\forall x \in I$, $\forall a \in A$.

$$I \cdot J = \left\{ \sum_{i=1}^{m} x_i y_i \;\middle|\; x_i \in I, y_i \in J \right\}.$$

Def. Dizemos que um ideal $I \subseteq A$ é:

(i) maximal se dado ideal J, com $I \subseteq J \subseteq A$, tem-se que $J = I$ ou $J = A$,

(ii) primo se dados ideais $I_1, I_2 \subseteq A$ com $I_1 \cdot I_2 \subseteq I$, segue que $I_1 \subseteq I$ ou $I_2 \subseteq I$.

Obs. Dado um ideal $I \subseteq A$, pode-se construir o anel quociente A/I.

Lema. Seja $I \subseteq A$ ideal.

(i) I é maximal $\Leftrightarrow$ A/I é corpo,

(ii) I é primo $\Leftrightarrow$ A/I é domínio.

Lema. Seja A um anel comutativo (com 1). Então A é corpo se e só se seus únicos ideais são 0 e A.

Def. Sejam A e B anéis e $f: A \to B$ função. Dizemos que f é homomorfismo de anéis se

(i) $f(a+b) = f(a) + f(b)$, $\forall a, b \in A$

(ii) $f(ab) = f(a)f(b)$, $\forall a, b \in A$.

Para nós: homomorfismo entende-se que $f(1_A) = 1_B$.

Obs. Seja $f: A \to B$ homomorfismo. Então $\ker f = \{a \in A \mid f(a) = 0\}$ é ideal e $f(A) = \{f(a) \mid a \in A\}$ é subanel.

Def. Um isomorfismo $f: A \to B$ é um homomorfismo bijetor (i.e. injetor e sobrejetor). Se f é um isomorfismo, então dizemos que A e B são isomorfos, e denotamos $A \cong B$.

Obs. $f: A \to B$ é injetor $\iff \ker f = 0$.

Teorema. Dado $f: A \to B$ homomorfismo, então

$$A/\ker f \cong f(A).$$

Além disso, existe bijeção entre os ideais de A contendo $\ker f$ e os ideais de $f(A)$.