Extensões Algébricas - $DAMCTB014 - 17SA$

- Docente: Edson Ryoji Okamoto Iwaki
    1. turma A-diurno- SA-QS2022.2.
    2. email: edson.iwaki@ufabc.edu.br

Atendimento aos discentes: A ser definido com a turma.
Objetivo: Introduzir os conceitos introdutórios da Teoria de Corpos e aplicações.
Horário:

- Terças-feiras: 8:00h-10:00h (semanal)
- Quinta-feiras: 10:00h-12:00 (semanal)

As reuniões serão realizadas através de uma plataforma digital:
Link para videoconferência: https://conferenciaweb.rnp.br/webconf/edson-60

Ementa:

Extensões finitas. Extensões algébricas. Extensões separáveis. Corpos Finitos. Extensões normais. Teoria de Galois. Extensões ciclotômicas. Solução por meio de radicais. Construção com régua e compasso. Extensões Transcendentes.

Estrutura do curso, Cronograma, Datas e Critérios de Avaliação

O curso será ministrado na forma remota e terá duração de 12 semanas com início no dia 06/06/2022.

Estrutura do Curso

Cronograma

A seguinte tabela mostra, para cada aula, o tópico que será tratado em ela. Este cronograma é aproximado podendo sofrer pequenas alterações durante o quadrimestre.

- Aula 1: Revisão: Corpo, característica de um anel. Característica de um corpo é zero ou prima. Corpo de frações de um domínio de integridade. Unicidade do corpo de frações de um domínio de integridade a menos de isomorfismo. Exemplos. Corpos primos. Todo corpo contém uma cópia de $\mathbb{Q}$ ou de $\mathbb{F}_p$ para algum primo p. Definição de extensão de corpos. Todo corpo é uma extensão de $\mathbb{Q}$ ou de $\mathbb{F}_p$.

- Aula 2: Teorema de Kronecker: Todo polinômio irredutível em $F[x]$ possui uma raiz em alguma extensão de corpos de F. Seja $p(x)$ pol. Irredutível sobre F de grau n e $O \equiv xmod(p(x))$ então $\{1, O, O^2, ..., O^{n-1}\}$ é base de K sobre F, onde $K = F[x]/ < p(x) >$. Revisão: R anel comutativo, R/I corpo se e somente se I é ideal maximal; R/P domínio de integridade se e somente se P é ideal primo de R. São equivalentes: (i) $p(x)$ irredutivel sobre F (ii) $< p(x) >$ ideal maximal de $F[x]$ (iii) $F[x]/ < p(x) >$ corpo. Revisão dos critérios de irredutibilidade de polinômios: Eisenstein, etc.

- Aula 3: Cálculos em $F[x]/ < p(x) >$, com $p(x)$ pol. Irred. Sobre F. Corpo gerado por uma família de elementos. Seja K/F extensão de corpos, $p(x)$ pol.irred. Sobre F e α raiz de $p(x)$ em L. Então $F(\alpha) \cong F[x]/ < p(x) >$. Caracterização de $F(\alpha)$.

- Aula 4: O Teorema de Extensão de Isomorfismo de corpos. Def. elemento algébrico sobre um corpo F. Def. Elemento transcendente sobre um corpo F. Exemplos. Extensão algébrica. Def. e exemplos. Existência e definição do polinômio minimal que possui um elemento α como raiz. O grau do elemento α. A extensão $F(\alpha)/F$ é finita se e somente se α é algebrico sobre F. Toda extensão finita é algébrica. $F \subset K \subset L$ corpos. Então $[L : F] = [L : K][K : F]$. Aplicações.

- Aula 5: Extensão finitamente gerada. Definição. L/K extensão finita se e somente se L é gerada por um número finito de elementos algébricos sobre K. L/K extensão então o conjunto dos elementos algébricos sobre K é um subcorpo. L/K extensão algebrica e K/F ext. algébrica então L/F é extensão algébrica. O compositum de dois subcorpos de um corpo. Corpos de decomposição e corpos algebricamente fechados.

- Aula 6: Exemplos de corpos de decomposição. Corpos ciclotômicos. Unicidade dos corpos de decomposição.
- Aula 7: Extensões separáveis e inseparáveis. Elemento separável numa extensão. Derivada formal de um polinômio. Critério para que uma raiz de um polinômio seja múltipla utilizando a derivada formal.Todo polinômio sobre um corpo de caracteristica zero é separável.
- Aula 8: Endomorfismo de Frobenius. Corpo perfeito definição. Existência e unicidade de corpos finitos. Definição L/K extensão separável.
- Aula 9: Extensões ciclotômicos. Irredutibilidade do $n-$ésimo polinômio ciclotômico. O Teorema do Elemento primitivo.
- Aula 10: Construções com régua e compasso. Os três grandes problemas da antiguidade
- Aula 11: L/K extensão. Def. de $Aut(L/K).Aut(L/K)$ permuta as raízes de polinômios irredutíveis.Exemplos. $H < Aut(K)$. Os elementos de K fixados por H são um subcorpo de K. (subcorpo fixo). Relação entre torres de subcorpos de K e subgrupos de $Aut(K)$.
- Aula 12: E corpo de decomposição sobre F do pol. $f(x) \in F[x]$. Então $|Aut(E/F)| \leq [E : F]$ com igualdade se $f(x)$ for separável sobre F. Extensão Galoisiana. Exemplos.
- Aula 13: O Teorema Fundamental da Teoria de Galois. Caracteres.
- Aula 14: O Teorema Fundamental da Teoria de Galois. Caracteres.
- Aula 15: Exemplos.
- Aula 16: Grupos de Galois de polinômios.
- Aula 17: Grupos de Galois de polinômios.
- Aula 18: Extensões radicais. Insolubilidade da quintica.

- Aula 19: Extensões radicais. Insolubilidade da quintica.
- Aula 20: Revisão da Matéria.

Metodologia

Nos horários síncronos das aulas serão discutidos os tópicos apresentados na ementa (por videoconferência), momento no qual eventuais dúvidas dos alunos poderão ser esclarecidas. Todas as informações sobre a disciplina estarão disponíveis na página da disciplina, a citar,

hostel.ufabc.edu.br/∼edson.iwaki/?page_id=1235.

Avaliação

- Os alunos serão avaliados por meio de 2 (duas) provas dissertativas. A cada uma destas avaliações será atribuída uma nota de 0 (zero) a 10 (dez). A duração de cada prova será de 24 horas. As mesmas deverão ser respondidas e as resposta escaneadas deverã o ser enviadas por email ao docente.

Tabela 1: Data das avaliações

Avaliação	**Data**
P1	14/07
P2	25/08

Conceitos

Será atribuída uma nota de de 0 (zero) a 10 (dez) a cada umas das avaliações. A média final será dada por

$$M = \frac{P1 + P2}{2},$$

onde $P1$ indica a nota da prova 1 e $P2$ denota a nota da prova 2.

Os conceitos serão atribuídos de acordo com a tabela abaixo:

Tabela 2: Conceitos

Conceito	**Intervalo**
A	$M \geq 8.5$
B	$7 \leq M < 8.5$
C	$5 \leq M < 7$
D	$4.5 \leq M < 5$
F	$M < 4.5$

Exame de recuperação

Será aplicado um exame de recuperação que englobará todo o conteúdo da disciplina. Caso o aluno opte por fazer o exame de recuperação, sua média final, MF , será dada por:

$$MF = \frac{M + R}{2},$$

onde R corresponde a nota obtida no exame de recuperação. A média final, MF , gerará um novo conceito, o qual será atribuído de acordo com a tabela acima.

Tabela 3: Data do exame de recuperação

Prova	**Data**
REC	19/09

De maneira similar as provas P1 e P2, o aluno terá 24h para entregar o exame de recuperação. A solução da mesma deverá ser enviada escaneada por email ao docente.

Bibliografia Básica

- ARTIN, E.; MILGRAM, A. N. Galois Theory. Mineola, NY: Dover Publications, 1998.
- EDWARDS, H. Galois Theory. New York: Springer-Verlag, 1984
- ENDLER, O. Teoria dos Corpos. Rio de Janeiro: IMPA, 2005
- JACOBSON, N. Basic Algebra I. 2nd ed. Mineola, NY: Dover Publications, 2009.
- KATZ, V. J.; FRALEIGH, J. B. A first course in abstract algebra. 7th ed. Boston: Addison- Wesley, 2003.

Bibliografia complementar

- DUMMIT, D. S.; FOOTE, R. M. Abstract Algebra. 3rd ed. Hoboken: Wiley, 2004.
- JACOBSON, N. Basic Algebra II. 2nd ed.Mineola, NY: Dover Publications, 2009.
- KAPLANSKY, I. Introdução à Teoria de Galois. Rio de Janeiro: IMPA, 1966.
- LANG, S. Algebra. 3rd ed. New York: Springer-Verlag, 2002.
- STEWART, I. Galois Theory. 3rd ed. Boca Raton: Chapman and Hall/CRC, 2003.
- VINBERG, E. B. A course in algebra. Providence, RI: American Mathematical Society, 2003