UNIVERSIDADE FEDERAL DO AMAZONAS

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

DEPARTAMENTO DE APOIO À PESQUISA

PROGRAMA DE BOLSAS DE INICIAÇÃO CIENTÍFICA

Relatório Final

RIGOR CIENTÍFICO EM ÁLGEBRA PURA – TEORIA DE GALOIS E MÓDULOS

PROGRAMA DE INICIAÇÃO CIENTÍFICA-UFAM

Miqueias de Melo Lobo, FAPEAM

MANAUS-2010

UNIVERSIDADE FEDERAL DO AMAZONAS

PRÓ-REITORIA DE PESQUISA E PÓS GRADUAÇÃO

DEPARTAMENTO DE APOIO À PESQUISA

PROGRAMA DE BOLSAS DE INICIAÇÃO CIENTÍFICA

Relatório Final

PIB-E-0036/2009-2010

ROGOR CIENTÍFICO EM ÁLGEBRA PURA – TEORIA DE GALOIS E MÓDULOS

PROGRAMA DE INICIAÇÃO CIENTÍFICA - UFAM

Miqueias de Melo Lobo, FAPEAM

Orientador: Prof. Dr. Claudenir Freire Rodrigues

MANAUS-2010

Sumário

1 INTRODUÇÃO

O objetivo desse projeto é mostrar a Correspondência de Galois. Para isto serão dadas as definições de Grupos, Subgrupos, Homomorfismo, Anéis, Polinômios, Extensões Algébricas e Espaços Vetoriais. Embora esta parte básica da teorias de grupos, anéis e polinômios seja considerada elementar, para que as idéias sobre o assunto fiquem bem estruturadas no sentido de não deixar de mencionar definições, estes conteúdos ainda assim estarão contidos no relatório. Por uma questão de simplicidade algumas proposições deixarão de ser demonstradas, mas isto não irá tirar a clareza nem o rigor do assunto abordado. Neste relatório também estão contidos o cronograma de atividades desenvolvidas e as referências bibliográficas que foram indispensáveis para a elaboração do mesmo.

2 TEORIA DOS GRUPOS

2.1 Grupos

Seja P um conjunto *não-vazio* no qual está definida uma operação entre seus pares, denotada por:

$$\begin{gathered} \cdot : P \times P \longrightarrow P \\ (a, b) \mapsto a \cdot b \end{gathered}$$

Se P cumpre as propriedades **(i), (ii)** e **(iii)** abaixo, então $(P, \cdot)$ é grupo.

(i) $u \cdot (v \cdot w) = (u \cdot v) \cdot w \ \forall \ u, v, w \in P$ (associatividadade)

(ii) $\exists \ e \in P$ tal que $u \cdot e = e \cdot u$ (elemento neutro)

(iii) $\forall \ u \in P, \exists \ v \in P$ tal que $u \cdot v = v \cdot u = e$ (inverso)

Se em $(P, \cdot)$ verifica-se a propriedade:

(iv) $a \cdot b = b \cdot a, \forall \ a, b \in G,$

dizemos que $(P, \cdot)$ é um grupo abeliano ou comutativo.

2.2 Subgrupos

Seja $(G, \cdot)$ um grupo. Um subconjunto $H \subset G$ é um *subgrupo* de G se, com a operação de G, o cunjunto H também é grupo. (denota–se $H \leq G$)

Uma outra forma de afirmar que certo conjunto $H \subset G$ é um subgrupo de G, é verificando se vale a seguinte proposição:

Proposição: Se $H \subset G$, $H \neq \emptyset$ e $\forall \, a, b \in H, ab^{-1} \in H$, então $H \leq G$.

Demonstração: Como $H \neq \emptyset$, então existe α tal que $e = \alpha\alpha^{-1} \in H$. Os elementos de H associam, pois isto vale para todos os elementos de G. A existência do inverso é dada por hipótese. Portanto $H \leq G$.

2.3 Classes Laterais

Seja G um grupo e seja H um subgrupo de G. Sobre G, defina a relação de equivalência $\sim$ da seguinte maneira:

$$y \sim x \Leftrightarrow \exists\, h \in H \;\; tal \;\; que \;\; y = xH$$

Por definição a classe de equivalência que contém x é o conjunto $\{y \in G \,|\, y \sim x\} = \{xh \,|\, h \in H\}$; denotaremos este conjunto por xH e chamaremos de *classe lateral de x à esquerda*.

2.4 Subgrupos Normais

O conjunto H é um *subgrupo normal* de G (escrevemos $H \triangleleft G$) se ele satisfaz as seguintes afirmações:

(i) $gHg^{-1} \subseteq H, \forall\, g \in G.$

(ii) $gHg^{-1} = H, \forall\, g \in G.$

(iii) $gH = Hg, \forall\, g \in G.$

As afirmações acima são todas equivalêntes. Neste caso as classes laterais à esquerda de H são iguais às classes laterais à direita de H, desta forma vamos chamá–las apenas de *classes laterais* de H.

2.5 Grupos Quocientes

Definição: Sejam G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais com a operação induzida de G é o *grupo quociente* de G por H. Ele será denotado por $\dfrac{G}{H}$.

2.6 Homomorfismo de Grupos

Definição: Sejam $(S, \bullet)$ e $(T, \circ)$ dois grupos. Uma função $f : S \to T$ é um *homomorfismo* se ela respeita a seguite regra:

$$f(x \bullet y) = f(x) \circ f(y), \;\; \forall\, x, y \in S.$$

2.6.1 Exemplo

1. $Id : (S, \bullet) \to (S, \bullet), Id(s) = s$, é um homomorfismo chamado *identidade*.

2.6.2 Propriedades Básicas

Seja $f : (S, \bullet) \to (T, \circ)$ um homomorfismo de grupos, então:

1. $f(e_S) = e_T$

2. $f(x^{-1}) = f(x)^{-1}$

3. $Kerf := \{p \in S \,|\, f(p) = e_T\}$ é um subgrupo normal de G chamado *núcleo* do homomorfismo f.

Demonstração: Primeiramente vamos verificar que $Kerf \leq S$. Pelo item 1, $Kerf \neq \emptyset$. Agora, dados $a, b \in Kerf$ temos que $f(a \bullet b^{-1}) = f(a) \circ f(b^{-1}) =$ $= f(a) \circ f(b)^{-1}$ (pelo item 2). Daí, $f(a) \circ f(b)^{-1} = e \circ e^{-1} = e$. Portanto, $ab^{-1} \in Kerf \Rightarrow Kerf \leq S$.

Agora, para provar que $Kerf \triangleleft S$ devemos mostrar que:

$$g \circ x \circ g^{-1} \in Kerf, \ \forall\, g \in S \ \ e \ \ \forall\, x \in Kerf$$

De fato, temos $f(g \circ x \circ g^{-1}) = f(g) \bullet f(x) \bullet f(g^{-1}) = f(g) \bullet e_T \bullet f(g)^{-1} =$ $= f(g) \bullet f(g)^{-1} = e_T$. Portanto, $Kerf \triangleleft S$.

4. $Imf = \{j \in T \,|\, j = f(i)$ para algum $i \in S\}$ é um subgrupo de T, chamado *imagem* de f.

Observação: Dois grupos G e G^* são ditos *isomorfos* se existe um homomorfismo bijetor de G em G^*. Neste caso escrevemos $G \simeq G^*$. Um *isomorfismo* de um conjunto S em si próprio é chamado de *automorfismo*. (escreve-se: Aut S)

Corolário 1. *Um homomorfismo φ de G em $\overline{G}$ com núcleo $ker\varphi$ é injetivo se, e somente se, $ker\varphi = \{e\}$.*

Demonstração: Sabemos que $\varphi(e) = e$. Tome $x \in ker\varphi$, então $\varphi(x) = e$. Como φ é injetiva e $\varphi(e) = \varphi(x) \Rightarrow e = x$. Reciprocamente, dados $a, b \in G$ tais que $\varphi(a) = \varphi(b)$, então $\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e$, então $ab^{-1} \in ker\varphi$. Como $ker\varphi = \{e\}$, $ab^{-1} = e \Leftrightarrow a = b$. Portanto φ é injetiva.

Corolário 2. *Seja f um homomorfismo sobrejetor de G em $\overline{G}$ com núcleo $kerf$, então $G/kerf \simeq \overline{G}$.*

Demonstração: Este é um caso particular do Teorema da Correspondência demonstrado abaixo.

2.7 Teorema da Correspondência

Seja $f : g \to H$ um homomorfismo de grupos. Existe uma bijeção:

$$\varphi : A = \{S \subset Imf \ ; \ S \leq Imf\} \longrightarrow B = \{T \subset G \ ; \ Kerf \subset T \leq G\}$$

$$S \mapsto f^{-1}(S)$$

Veremos que $f^{-1}(S)$ é subgrupo de G.
Se $S \leq Imf$, $\{e\} \subset S \Rightarrow Kerf = f^{-1}(\{e\}) \subset f^{-1}(S)$. Daí, $f(e) = e \in S \Rightarrow$
$\Rightarrow e \in f^{-1(S)}$. Portanto $f^{-1}(S) \neq \emptyset$.
Dados $a, b \in f^{-1}(S) \Rightarrow f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in S$. Daí, $ab^{-1} \in S$ e portanto $f^{-1}(S) \leq G$.

Agora, iremos verificar que a função φ é bijetiva.

Sejam $S_1, S_2 \leq Imf$ tal que $\varphi(S_1) = \varphi(S_2)$ então $f^{-1}(S_1) = f^{-1}(S_2)$.
Sabemos que $f : G \to Imf$ é sobrejetiva e $S_1, S_2 \subset Imf$. Logo $f\Big(f^{-1}(S_1)\Big) =$
$= f\Big(f^{-1}(S_2)\Big)$ então $S_1 = S_2$. Portanto φ é injetiva.

E φ é sobrejetiva, pois se $T \in B$, temos que $f(T) \leq Imf$. Veremos que $\varphi\Big(f(T)\Big) = T$, isto é, $f^{-1}\Big(f(T)\Big) = T$.

De fato, se $x \in f^{-1}\Big(f(T)\Big) \Rightarrow f(x) \in f(T)$, então existe $u \in T$ tal que $f(x) = f(u)$. Segue que $f(x)f(u^{-1}) = e \Rightarrow f(xu^{-1}) = e$ e isto implica que $xu^{-1} = h \in Kerf \Rightarrow x = hu \in T$. Portanto, $f^{-1}\Big(f(T)\Big) \subset T$.

E se $y \in T \Rightarrow f(y) \in f(T)$, isto implica que $y \in f^{-1}\Big(f(T)\Big)$. Daí, $T \subset f^{-1}\Big(f(T)\Big)$. Segue que, φ é sobrejetiva.
De φ ser injetiva e sobrejetiva, temos a bijetividade desta função.

Se $Kerf \subset T \leq G$ e T corresponde a $f(T) \leq Imf$.

Temos que a função

$$\varphi_T : \frac{T}{Kerf} = \{aKerf\,;\, a \in T\} \longrightarrow f(T)$$

$$(aKerf) \mapsto f(a)$$

é um isomorfismo.

De fato, se duas classes são iguais. Ou seja,
$aKerf = bKerf \Leftrightarrow ab^{-1} \in Kerf \Rightarrow f(ab^{-1}) = e \Rightarrow f(a)f(b)^{-1} = e \Rightarrow$
$\Rightarrow f(a) = f(b)$.
... então os representantes são iguais. Portanto, φ_T é bem definida no sentido de não depender da escolha do representante.

Resta ver que φ_T é um homomorfismo bijetivo.

$\varphi_T(aKerf \cdot bKerf) = \varphi_T(abKerf) = f(ab)$. Como f é homomorfismo, vale que $f(ab) = f(a)f(b) = \varphi_T(aKerf) \cdot \varphi_R(bKerf)$.

Se
$\varphi_T(aKerf) = e \Rightarrow f(a) = e \Rightarrow a \in Kerf \Leftrightarrow aKerf = Kerf = e_{T/Kerf}$.
então φ_T é injetiva.

E, se
$a \in T \Rightarrow a = f(u)$ tal que $u \in T$, então $f(u) = \varphi_T(uKerf)$
então φ_T é sobrejetiva. E isso conclui a demonstração do Teorema.

3 TEORIA DOS ANÉIS

Definição: Um conjunto não-vazio R é dito um *anel* se nele estão definidas duas operações simbolizadas por $+$ e $\cdot$, respectivamente, tais que para todos a, b e c em R vale:

(1) $a + b \in R$

(2) $a + b = b + a$

(3) $(a + b) + c = a + (b + c)$

(4) Existe $0 \in R$ tal que $a + 0 = a$ (para cada $a \in R$)

(5) Dado $a \in R$ existe $-a \in R$ tal que $a + (-a) = o$

(6) $a \cdot b \in R$

(7) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(8) $a \cdot (b + c) = a \cdot b + a \cdot c$

Pode muito bem acontecer, ou não acontecer, que exista um elemento $1 \in R$ tal que $a \cdot 1 = a$ para todo $a \in R$. Se existe tal elemento, R é denominado *anel com unidade*. Se o produto de R é tal que $a \cdot b = b \cdot a$ para todos $a, b \in R$, então chamamos R de *anel comutativo*. Notamos que, sendo R um anel, $(R, +)$ é grupo abeliano. Se os elementos de R diferentes de 0 formam um grupo abeliano com a operação $\cdot$, então dizemos que R é um *corpo*. Um anel comutativo é dito *domínio de integridade* se não possui divisores do zero, isto é, se $a, b \in R$ com $ab = 0$, então $a = 0$ ou $b = 0$.

3.1 Subanéis

Um conjunto não-vazio S de um anel A é um *subanel* de A se S for um anel com as operações de A.

Proposição: *Um subconjunto S de um anel A é um subanel de A se:*

(i) $S \neq \emptyset$

(ii) Para todo $a, b \in S$, $a - b \in S$ e $ab \in S$

Demonstração: Como as propriedades comutativa, associativa, distributiva são válidas para A, em particular, para S. Então faltam apenas verificar se são fechadas, se o elemento neutro está em S e se o inverso aditivo de cada elemento de S está em S. Por hitótese, se $a, b \in S$ então $ab \in S$. Como $S \neq \emptyset$, tome $x \in S$. Por hipótese $x - x = 0 \in S$. Também, por hipótese $0 - a = -a \in S$ para todo $a \in S$. Logo, se $a, b \in S$, $a + b = a - (-b) \in S$ e isto termina a demonstração.

3.2 Ideais

Um subanel I de um anel A é chamado um *ideal* de A se para todo $a \in A$ e todo $x \in I$, $xa \in I$.

Assim, um subanel de um anel A é um ideal se ele absorve os elementos de A, isto é, $aI \subseteq I$ para todo $a \in A$. Um ideal é dito *próprio* se $I \neq A$.

Proposição: *Um subconjunto I, não-vazio, de um anel A é um ideal se:*

(i) $a - b \in I$, para todo $a, b \in I$

(ii) $xa \in I$ quando $a \in A$ e $x \in I$

Um ideal é dito principal quando for gerado por um elemento. (semelhante aos grupos cíclicos)

3.3 Anéis Quocientes

Seja A um anel e I um ideal de A. Defina em A e relação:

$$x \sim y \Leftrightarrow x - y \in I$$

É fácil ver que $\sim$ é uma relção de equivalência. Assim, como toda relação de quivalência determina uma partição temos que A vai ser a reunião disjunta das classes de equivalência:

$$A = \bigcup_{x \in A} \overline{x}$$

onde $\overline{x} = \{y \in A \mid y \sim x\} = \{y \in A \mid y \in x + I\}$. A classe $\overline{x}$ será representada por $x + I$ e $A/I = \{x + I \mid x \in A\}$. A/I é um anel com a mesma operação definida para grupos.

3.4 Ideais Maximais

Um ideal $J \neq A$ em um anel R é dito *maximal* de A se sempre que L for um ideal de A tal que $J \subset L \subset A$, então $L = A$ ou $L = J$.

Teorema 1. *Seja A um anel comutativo com unidade $1 \in A$ e seja J um ideal de A. Então J é maximal de A se, e somente se, A/J é um corpo.*

Demonstração: Suponha que J seja maximal em A, e seja $\overline{0} \neq \overline{a} \in A/J$. Veremos que existe $\overline{b} \in A/J$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. De fato, se $L = A \cdot a$ é um ideal principal gerado por a, temos que $J + L = \{x + y \mid x \in J,\ y \in L\}$ é um ideal contendo J, e mais $\overline{a} \neq \overline{0} \Leftrightarrow a \notin J$. Como $a = 1 \cdot a \in L \subset J + L$ temos que $J + L$ é um ideal que contém J e $J + L \neq J$. Pela maximalidade de J segue que $A = J + L$ e daí vem, $1 \in J + L \Rightarrow \exists\ u \in J,\ v \in L$ tais que $1 = u + v$. Mas $v \in L = A \cdot a$ e temos que $v = b \cdot a$ para algum $b \in A$, ou seja, existem $b \in A$ e $u \in J$ tais que $1 = u + b \cdot a$.
Tomando acasse deste objeto, teremos $\overline{1} = \overline{u + b \cdot a} = \overline{u} + \overline{b} \cdot \overline{a} = \overline{0} + \overline{b} \cdot \overline{a} = \overline{b} \cdot \overline{a}$, como queríamos.

Reciprocamente, suponha que A/J seja um corpo. Assim, $\overline{0}, \overline{1} \in A/J \Rightarrow J \neq A$. Se $M \neq J$ é um ideal de A e $J \subset M \subset A$, então teremos que existe $a \in M$, $a \notin J$, ou seja, $\overline{a} \neq \overline{0}$, $\overline{a} \in A/J$. Como A/J é corpo existe $\overline{b} \in A/J$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, ou melhor, $ab - 1 \in J \Leftrightarrow \exists\ u \in J$ tal que $ab - 1 = u \Leftrightarrow 1 = ab - u$. Como $a \in M \Rightarrow ab \in M$ e como $u \in J \subset M \Rightarrow u \in M$. Logo $1 = ab - u \in M$ e segue imediatamente que $M = A$.

3.5 Homomorfismos de Anéis

Sejam A e B dois anéis. Uma função $f : A \to B$ diz-se um *homomorfismo* de A em B se satisfaz as seguintes condições:

(i) $f(x + y) = f(x) + f(y)$ para quaisquer $x, y \in A$

(ii) $f(x \cdot y) = f(x) \cdot f(y)$ para quaisquer $x, y \in A$

3.6 Anéis de Polinômios

Seja F um corpo. Por *anel de polinômio* na indeterminada x, indicado por $F[x]$, entendemos o conjunto de todos os símbolos $a_0 + a_1x + \cdots + a_nx^n$, onde n pode ser qualquer inteiro não negativo e onde os coeficientes $a_0, a_1, \cdots, a_n$ estão todos em F.

Definição 1: Se $p(x) = a_0 + a_1x + \cdots + a_mx^m$ e $q(x) = b_0 + b_1x + \cdots + b_nx^n$ estão em $F[x]$, então $p(x) = q(x)$ se, e somente se, para todo inteiro $i \geq 0$, $a_i = b_i$.

Assim, dois polinômios são ditos iguais se, e somente se, seus coeficientes correspondentes são iguais.

Definição 2: Se $p(x) = a_0 + a_1x + \cdots + a_mx^m$ e $q(x) = b_0 + b_1x + \cdots + b_nx^n$ estão ambos em $F[x]$, então $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$, onde para cada i, $c_i = a_i + b_i$.

Em outras palavras, somamos dois polinômios somando seus coeficientes e colecionando seus termos.

Definição 3: Se $p(x) = a_0 + a_1x + \cdots + a_mx^m$ e $q(x) = b_0 + b_1x + \cdots + b_nx^n$, então $p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_kx^k$, onde $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-1}b_2 + \cdots + a_0b_t$.

Esta definição não diz nada mais que: multiplicamos dois polonômios multiplicando os termos formalmente, usando a relação $x^mx^n = x^{m+n}$ e colecionando os termos. Se $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ e $a_n \neq 0$, então o *grau* de $f(x)$, indicado por $gr\, f(x)$, é n. Isto é, o grau de $f(x)$ é o maior natural i para o qual i i-ésimo coeficiente de $f(x)$ não é 0.

Lema 1: *Se $f(x), g(x)$ são dois elementos não nulos de $F[x]$, então $gr[f(x)g(x)] = gr\, f(x) + gr\, g(x)$.*

Lema 2 (Algorítmo da Divisão): *Dados dois polinômios $f(x)$ e $g(x) \neq 0$ em $F[x]$, então existem dois polinômios $t(x)$ e $r(x)$ em $F[x]$ tais que $f(x) = t(x)g(x) + r(x)$ onde $r(x) = 0$ ou $gr\, r(x) < gr\, g(x)$.*

Definição 4: Um polinômio $p(x) \in F[x]$ é dito *irredutível* sobre F se sempre que $p(x) = a(x)b(x)$, com $a(x)$, $b(x) \in F[x]$, então $a(x)$ ou $b(x)$ tem grau 0, isto é, é uma constante.

Lema 3: Qualquer polinômio em $F[x]$ pode ser escrito de uma única maneira como produto de polinômios irredutíveis em $F[x]$.

4 EXTENSÕES ALGÉBRICAS

Agora, K representa um corpo e $L \supset K$ um extensão de K. Dizemos que $a \in L$ é *algébrico* sobre K se exite $f(x) \in K[x] - \{0\}$ tal que $f(a) = 0$. Caso contrário dizemos que a é *transcendente* sobre K. Se $a \in K$, evidentemente a é algébrico sobre K pois é raiz do polinômio $g(x) = x - a \in K[x]$.
Se para todo $a \in L \supset K$, a é algébrico sobre K, então $L \supset K$ diz-se uma *extensão algébrica*.

4.1 Corpo de decomposição de um polinômio

Chamamos de *corpo de decomposição de um polinômio* $f(x) \in K[x]$ sobre K, que será denotado por $L = Gal(f, K)$ ao menor subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$. Tal menor subcorpo existe e é igual a interseção de todos os subcorpos de $\mathbb{C}$ contendo K e todas as raízes de $f(x)$ em $\mathbb{C}$.

4.2 Índice ou grau de uma extensão

Antes de tudo, algumas noções de Álgebra Linear como espaços vetoriais e bases serão dadas.

Seja K um corpo qualquer e seja V um conjunto não vazio onde stá definida uma operção soma. Soponhamos também que esteja definida uma operação de elementos de K por um elemento de V.
Dizemos que V munido dessas operações é um *espaço vetorial sobre o corpo* K se as seguintes propriedades são verificadas quaisquer que sejam $u, v, w \in V$ e $\lambda \in K$:

(1) $u + (v + w) = (u + v) + w$

(2) $\exists\, 0 \in V$ tal que $u + 0 = 0 + u = u$

(3) $\forall\, x \in V, \exists\, y \in V$ tal que $x + y = y + x = 0$

(4) $u + v = v + u$

(5) $1v = v$ onde 1 é a unidade do corpo K

(6) $\lambda(u + v) = \lambda u + \lambda v$ e $(\lambda_1 + \lambda_2)u = \lambda_1 u + \lambda_2 u$

(7) $\lambda(uv) = (\lambda u)v$

Se $L \supset K$ é um extensão, L pode ser visto como um espaço vetorial sobre K pois as operações de soma e produto existem de modo natural no corpo L.

Subespaço
Um subconjunto não vazio W de V diz-se um *subespaço vetorial de* V se as seguinte condições são satisfeitas:

(i) $w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$

(ii) $\lambda \in K, w \in W \Rightarrow \lambda w \in W$

Se $v_1, \cdots, v_n \in V$ dizemos que $v_1, \cdots, v_n$ são *lenearmente independentes* se a combinação $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0, \alpha_i \in K$ é satisfeita apenas para os escalares $\alpha_1 = \cdots = \alpha_n = 0$. Caso contrário dezemos que os vetores $v_i's$ são *linearmente dependentes.*Usaremos L.I. para linearmente dependente e L.D. para linearmente dependentes.
Se $u_1, \cdots, u_r \in V$ então $W = \{\alpha_1 + \cdots + \alpha_r \ : \ \alpha \in K\}$ é um espaço vetorial, o qual chamaremos de *subespaço gerado* por $u_1, \cdots, u_r$. Denotaremos este espaço por:

$$W = \langle u_1, \cdots, u_r \rangle$$

Se o conjunto $v_1, \cdots, v_n \in V$ for L.I. e tal que $V = \langle v_1, \cdots, v_n \rangle$ dizemos que $v_1, \cdots, v_n$ é uma base de V.

Teorema 1:(a) *Todo espaço vetorial* V *sobre um corpo* K *possui uma base.* (b) *Se um espaço vetorial* V *sobre um corpo* K *possui uma base com* n *elementos, então toda base de* V *possui* n *elementos.*

Se um espaço vetorial V sobre um corpo K possui uma base com n elementos, chamamos ao número n de *dimensão de* V *sobre* K e denotamos $[V : K] = n$.

Definição: Seja K um corpo qualquer. Uma extensão $L \supset K$ diz-se *finita* se $[L : K] = n < \infty$. Casa contrário $L \supset K$ diz-se uma *extensão infinita.*

5 CORRESPONDÊNCIA DE GALOIS

5.1 Extensões galoisianas e extensões normais

Dizemos que uma extensão finita é uma *extensão galoisiana* se $\exists\, f(x) \in K[x]$ tal que $L = Gal(f, K)$, e dizemos que uma extensão algébrica $L \supset K$ é normal se $\forall\, g(x) \in K[x]$, irredutível sobre K que possui uma raiz $\alpha \in L$ possui todas as suas raízes complexas em L.
Observe que se $L \supset M \supset K$ são extensões tais que $L \supset K$ é galoisiana então $L \supset M$ é também galoisiana.

Proposição 1: *Seja $L \supset K$ uma extensão finita. Então, $L \supset K$ é galoisiana $\Leftrightarrow$ $L \supset K$ é normal.*

Teorema 1: *Se $L \supset M \supset K$ são extensões finitas e $L \supset K$ é galoisiana, então as seguintes sfirmações são equivalentes:*

(a) $M \supset K$ *é galoisiana*

(b) $\sigma(M) \subseteq M,\ \forall\, \sigma \in Aut_M L$

(c) $Aut_M L \lhd Aut_K L$

Demonstração: $(a) \Rightarrow (b)$ - Seja $u \in L$ tal que $M = K[u]$. Se $M \supset K$ galoisiana segue da proposição 1 acima que $M \supset K$ é uma extensão normal. Agora, se $h = irr(u, K)$ e $\sigma \in Aut_K L$ sabemos que $v = \sigma(u)$ é também raiz de $h(x)$ e pela normalidade de $M \supset K$ temos $v = \sigma(u) \in M$, ou seja, $\sigma(K[u]) \subseteq K[u]$ como queríamos.

$(b) \Rightarrow (a)$ - Seja $u \in L$ tal que $M = K[u]$ e seja $h = irr(u, K)$. Vamos provar que se $\sigma(M) \subseteq M\ \forall\, \sigma \in Alt_K L$ temos $M = Gal(h, K)$. Seja v raiz de $h(x)$, e seja $M' = K[v]$. Existe um isomorfismo, $\sigma_0 : M \to M'$ tal que $\sigma(u) = v$ e $\sigma(a) = a\ \forall\, a \in K$. Existe, ainda, $\sigma \in Alt_K L$ tal que $\sigma|_M = \sigma_0$. Como $\sigma(M) \subseteq M$ e $u \in M$ teremos $v = \sigma(u) \in M$ como queríamos.

$(b) \Rightarrow (c)$ - Sejam $\sigma \in Aut_K L$ e $\gamma \in Aut_M L$. Vamos provar que se $\sigma(M) \subseteq M$ então $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$. De fato, se $\sigma(M) \subseteq M$ e $m' = \sigma(m), m \in M$ temos: $\gamma(m') = m'$ e $(\sigma^{-1} \circ \gamma \circ \sigma)(m) = \sigma^{-1}(\gamma(m')) = \sigma^{-1}(m') = m$ e isto demonstra a implicação.

$(c) \Rightarrow (b)$ - Suponhamos por absurdo que $\exists\, \sigma \in Aut_K L$ e $\exists\, u \in M$ tal que $\sigma(u) = v \notin M$. Como $L \supset K$ é galoisiana temos $L \supset M$ também galoisiana,

daí segue que: $\exists\, \gamma \in Aut_M L$ tal que $\gamma(v) \neq v$. Assim, $(\sigma^{-1} \circ \gamma \circ \sigma)(u) = \sigma^{-1}(\gamma(v)) \neq \sigma^{-1}(v) = u$ ou seja $\sigma^{-1} \circ \gamma \circ \sigma \notin Aut_M L$ contrariando a hipótese $Aut_M L \lhd Aut_K L$.

Teorema 2: *Seja $L \supset K$ uma extensão finita. Então as seguites condições são equivalêntes:*

(1) *$L \supset$ é galoisiana*

(2) *$L \supset K$ é normal*

(3) *$\forall\, \alpha \in L - K$, $\exists\, \sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$*

(4) $[L : K] = |Aut_K L|$

Seja $M \supset K$ uma extensão finita. Dezemos que L é um *corpo intermediário de $M \supset K$* se L é um subcorpo de M contendo K, ou seja $M \supset L \supset K$.
Se $G = Aut_K M$ usaremos as seguintes notações:

$$\mathfrak{I}(M, K) = \{L : corpo\ \ intermediario\ \ de\ \ M \supset K\}$$

$$\mathfrak{S}(G) = \{H : H \leq G\}$$

Se $H \in \mathfrak{S}(G)$ então $L = \{a \in M : \gamma(a) = a\ \forall\, \gamma \in H\}$ é corpo intermediário de $M \supset K$. De fato obviamente $0, 1 \in L$ e mais:

(i) se $x, y \in L$ então $\gamma(x - y) = \gamma(x) - \gamma(y) = x - y$, $\forall\, \gamma \in H$

(ii) se $x, y \in L$ então $\gamma(xy) = \gamma(x) \cdot \gamma(y) = xy$, $\forall\, \gamma \in H$

(iii) se $x \in L, x \neq 0$ então $\gamma(x^{-1}) = \gamma(x)^{-1}$, $\forall\, \gamma \in H$ e como $G = Aut_K M$ e $H \leq G$ segue imediatamente que L é um corpo, $M \supset L \supset K$. Esse corpo L é chamado *corpo fixo de H*

(Teorema fundamental de Galois) - *Se $M \supset K$ é uma extensão galoisiana, então:*

(a) *$\forall\, L \in \mathfrak{I}(M, K)$ tem-se $[M : L] = |\psi(L)|$ e $[L : K] = [G : \psi(L)]$ (o índice de $\psi(L)$ em G)*

(b) *$\forall\, H \in \mathfrak{S}(G)$ tem-se $[M : \theta(H) : K] = [G : H]$*

(c) *$\psi \circ \theta = I_{\mathfrak{S}(G)}$ e $\theta \circ \psi = I_{\mathfrak{I}(M,K)}$*

(d) $\forall\, L \in \mathfrak{I}(M,K),\ L \supset K$ *galoisiana* $\Leftrightarrow \psi(L) = Aut_L M \lhd G$

(e) *Seja* $L \in \mathfrak{I}(M,K)$. *Se* $L \supset K$ *galoisiana então* $[L:K] = |Aut_K L|$ *e* $G/\psi(L) \simeq Aut_K L$

Demonstração: (a) Seja $L \in \mathfrak{I}(M,K)$, $M \supset L \supset K$. Ora, $M \supset K$ galoisiana implica que $MsupsetL$ é galoisiana daí segue que:

$$[M:L] = |Aut_L M| = |\psi(L)|$$

e como $[M:K] = |Aut_K M| = [M:L]\cdot[L:K]$ temos que:

$$|G| = [M:L]\cdot[L:K] = |\psi(L)|\cdot[L:K]$$

e daí vem que: $[L:K] = [G:\psi(L)]$ como queríamos.

(b) Sejam$H \leq G$ e $L = \theta(H)$. Como $|G| = [M:K] = [M:\theta(H)]\cdot[\theta(H):K]$ então a fórmula $[\theta(H):K] = [G:H]$ segue imediatamente da primeira parte $[M:\theta(H)] = |H|$ e é essa que vamos demonstrar a seguir. Sabemos pelo item (a) que: $[M:L] = |\psi(L)|$ onde $L = \theta(H)$. Assim $[M:\theta(H)] = |\psi(\theta(H))|$ e portanto temos: $[M:\theta(H)] \geq |H|$. Suponhamos por absurdo que:

$$[M:\theta(H)] > |H|$$

e suponhamos que $H = \{\varphi_1 = I_M, \varphi_2, \cdots, \varphi_n\}$. Como $[M:\theta(H)] = [M:L] > n$ então existem $(n+1)$ vetores $u_1, \cdots, u_{n+1}$ que são L.I. sobre o corpo $L = \theta(H)$.

(c) Seja $H \in \mathfrak{S}(G)$ e $L \in \mathfrak{I}(M,K)$. Sabemos que $H \leq \phi(\theta(H))$ e $L \leq \theta(\psi(L))$. Pelo item (a), temos $[G:\psi(\theta(H))] = [\theta(H):K]$ e pelo item (b), temos: $[M:\theta(\psi(L))] = |\psi(L)|$ e pelo item (a) temos $|\psi(L)| = [M:L]$. Daí segue imediatamente que:

$$\theta \circ (\psi(L)) = L$$

Portanto fica demonstrado o item (c).

(d) Consequência imediata do Teorema 1

(e) Pelo item (a) sabemos que $[G:\psi(L)] = [L:K]$ portanto é suficiente provarmos que: $\forall\, L \in \mathfrak{I}(M,K) L \supset K$ galoisiana implica que:

$$G/\psi(L) \simeq Aut_K L$$

De fato, como $L \supset K$ galoisiana, sabemos pelo Teorema 1 que, $\forall\, \sigma \in G = Aut_K M$ tem-se $\sigma_0 = \sigma|_L \in Aut_K L$, portanto podemos definir a seguinte função:

$$\Phi : G \to Aut_K L \text{ onde } \Phi(\sigma) \mapsto \sigma_0 = \sigma|_L$$

Φ é evidentemente um homomorfismo de grupos, cujos núcleo $ker\Phi = \{\sigma \in G : \sigma_0 = \sigma|_L = I_L\} = Aut_L M = \psi(L)$.

Agora pelo Teorema da extensão sabemos que Φ é também sobrejetiva e o resto segue do 1º teorema do isomorfismo.

6 CONCLUSÃO

Dado um polinômio $p(x)$ em $F[x]$, o anel dos polinômios em x sobre F, associamos a $p(x)$ um grupo, denominado o *grupo de Galois* de $p(x)$. Agora percebemos que existe uma estreita relação entre as raízes de um polinômio e seu grupo de Galois. Na verdade o grupo de Galois é um certo grupo de permutações das raízes do polinômio. E o meio de introduzir este grupo foi através do corpo das rsízes do polinômio sobre F, o grupo de Galois sendo definido como um certo grupo de autumorfismos deste corpo de raízes. Vimos que existe um bela dualidade, expressa no teorema fundamental de Galois, entre os grupos de Galois e os subcorpos do corpo de raízes.

7 CRONOGRAMA

O desenvolvimento do projeto obedece o seguinte cronograma:

Atividades	Fev - 2010	Mar	Abr	Mai	Jun	Jul
Aulas de Polinômios e Extensões				X	X	X
Aulas de Teoria de Galois			X	X	X	X
Estudo dirigido pelo orientador	X	X	X	X	X	X
Elaboração do Relatório Final						X

8 BIBLIOGRAFIA

Referências

[1] Garcia, Arnaldo. Elementos de Álgebra. IMPA – Projeto Euclides.

[2] Hernstein, I.N. . Topics in Algebra. Blaisdell.

[3] Rotman, Joseph J.. An Introduction to the Theory of Groups. Springer

[4] Lang, Serge. Algebra. Springer