ON INTEGRAL BASES OF SOME RING OF INTEGERS

Nelo D. Allan

RELATÓRIO TÉCNICO Nº 10/88

SUMMARY. Let R be a Dedekind domain and K be its quotient field. Let L be a finite separable extension of K, with $L = K(x)$, x being in the integral closure S of R in L. We let $f(x) \in R[X]$ be the minimal monic polynomial of x, and let $\Delta = \Delta(x) = \Delta(f)$ be its discriminant. Let $D = D(S/K)$ be the discriminant of S over K. We show that under certain conditions $S = R[X]$ if and only if Δ is square free. Moreover if f remains irreducible over $E = K(y)$, $y^2 = \eta\Delta$, η unit of R, then $L(y)$ is unramified over E. Our conditions apply to the case where $f(X) = X^n - aX^k - b$, $a, b \in R$, with nb and $(n-k)ka$ being relatively prime and b being a unit if $k > 1$.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
BRASIL

Maio – 1988

1. INTRODUCTION

We let $\mathcal{L} \supset \mathcal{K}$ be the quotient fields of Dedekind domains $\mathcal{S}$ and $\mathcal{R}$, respectively, such that $\mathcal{L} = \mathcal{K}(x)$, $x \in \mathcal{S}$, $\mathcal{L}$ separable over $\mathcal{K}$, and $\mathcal{S}$ is the integral closure of $\mathcal{R}$ in $\mathcal{K}$. We let $f(X) \in \mathcal{R}[X]$ be the minimal monic polynomial or x over $\mathcal{K}$, say of degree $d^o f = n$ and $\Delta = \Delta(f) = \Delta(x)$ be its discriminant ; We set $D = D(\mathcal{S}/\mathcal{K})$ = the discriminant of $\mathcal{S}$ over $\mathcal{K}$. We say that $\mathcal{K}$ is an ANF, if it is an algebraic number field of finite degree over the rationals $\mathbb{Q}$ and $\mathcal{R}$ is the integral closure of $\mathbb{Z}$, the integers, in $\mathcal{K}$. We say that $\mathcal{K}$ is an AFF, if it is an algebraic function field such that $\mathcal{K}$ is a finite extension of $\mathcal{F}(X_o)$ with $\mathcal{F}$ finite and X_o transcendental over $\mathcal{F}$, and $\mathcal{R}$ is the integral closure of $\mathcal{F}[X_o]$ in $\mathcal{K}$. In both cases we say that $\mathcal{K}$ is a global field and in this case $D = D(\mathcal{S}/\mathcal{K})$ is the discriminant of $\mathcal{L}$ over $\mathcal{K}$. We know that $\mathcal{S}$ is an $\mathcal{R}$-lattice of rank n, and our problem is to find a bases $\{u_1,\ldots,u_n\}$ for $\mathcal{R}[x]$ and ideals $\mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \ldots \subseteq \mathcal{A}_n$, the invariant factors of S such that $S = \mathcal{A}_1u_1 + \ldots + \mathcal{A}_nu_n$. We denote by $t(i,j)$ the trace $T_r(\mathcal{L}/\mathcal{K})(x^{i+j})$ and the $T = (t(i,j))$, $0 \leq i,j \leq n-1$. Let $T(m,j)$ be the cofactor of $t(j,m)$ in T, and $z = z(m) = \Sigma\{T(m,j)x^j \mid 0 \leq j \leq n-1\}$. Also by g.c.d.$(a,b)$, $a,b \in \mathcal{R}$, we mean the greatest common divisor of a and b.

THEOREM 1: Let us assume that we can find a pair (m,j) such that Δ and $T(m,j)$ are relatively prime.

Then

(a) $\mathcal{S} = \mathcal{R}[x]$ if and only if $\Delta = D(\mathcal{S}/\mathcal{K})$ is square free.

(b) If $(\Delta) = \mathcal{A}^2\mathcal{B}$, $\mathcal{A},\mathcal{B}$ ideals in $\mathcal{R}$, $\mathcal{B}$ square free, then $\mathcal{S} = \mathcal{R} + \ldots + \mathcal{R}x^{n-1} + \mathcal{A}^{-1}z$ with the term in x^j being ommited. Consequently $D(\mathcal{S}/\mathcal{K}) = \mathcal{B}$

(c) If $\mathcal{K}$ is a global field and f remains irreducible over $\mathcal{E} = \mathcal{K}(y)$, $y^2 = \eta\Delta$, η unit of $\mathcal{R}$, then both $\mathcal{L}^* = \mathcal{L}(y)$ and the sppliting field $\mathcal{E}^*$ of f over $\mathcal{E}$, are unramified over $\mathcal{E}$.

This theorem generalizes Uchida's Theorem 1 (Uchida, 1970).

As an application of this theorem we have:

THEOREM 2: If $f(X) = X^n - aX^k - b$, $a,b \in \mathcal{R}$, f irreducible over $\mathcal{K}$ and $(n-k)ka$, nb being relatively prime with b unit if $k > 1$. Then hypothesis of theorem 1 are satisfied.

For $k = 1$, this theorem generalizes some of the results of Komatsu (Komatsu, 1975). Also treated by the author (Allan, 1982).

A special case where all the assumptions of theorem 1 hold is given by $f(X) = X^5 - aX^2 + 1$ $a \in \mathbb{Z}$, a odd. Here $\mathcal{L}' = \mathbb{Q}(x,y)$ is unramified over $\mathcal{E} = \mathbb{Q}(y)$ and if $a = 1$, $\Delta = 7.431 = D(\mathcal{K}/\mathbb{Q})$ and $\mathcal{S} = \mathbb{Z}[x]$.

This note contains the proof announced in our forthcoming paper (Allan, 1988).

1. GENERALITIES ON DEDEKIND DOMAINS

In this paragraph we shall review some well known properties on the arithmetics of Dedekind domains.

1.1. DEFINITION AND EXAMPLES

DEFINITION. Let $\mathcal{R}$ be a noetherian domain. We say that $\mathcal{R}$ is Dedekind domain if $\mathcal{R}$ satisfies the following equivalent conditions:

(a) $\mathcal{R}$ is integrally closed in its quotient field $\mathcal{K}$.

(b) All prime ideals of $\mathcal{R}$ are maximal.

(c) The $\mathcal{R}$-fractionary ideals of $\mathcal{R}$ form a multiplicative group.

By an $\mathcal{R}$-fractionally ideal we mean an $\mathcal{R}$-module $\mathcal{M}$ of $\mathcal{K}$ such that for some $a \in \mathcal{R}$, $a\mathcal{M} \subset \mathcal{R}$.

EXAMPLES:

(I) All fields and principal ideal domains are Dedekind. Also

THEOREM 1. Let $\mathcal{R}$ be a Ded-domain and $\mathcal{K}$ be its quotient field. Let $\mathcal{L}$ be a finite separable extension of $\mathcal{K}$ and $\mathcal{S}$ be the integral closure of $\mathcal{R}$ in $\mathcal{L}$. Then $\mathcal{S}$ is Dedekind.

From this we get:

(II) If $\mathbb{Q}$ = rationals ; $\mathbb{Z}$ = ordinary integers; $\mathbb{Z}$ is Dedekind and if $\mathcal{K}$ is a finite extension of $\mathbb{Q}$, then the integral closure $\mathcal{R}$ of $\mathbb{Z}$ in K is also Dedekind. We say that $\mathcal{K}$ is A.N.F. (Algebraic Number Field).

(III) Let $\mathbb{F}_q$ be the field with q elements, $q = p^{\ell}$, $\ell \geq 1$, and let X_o be transcendental over $\mathbb{F}_q$; we set $\mathcal{K}_o = \mathbb{F}_q(X_o)$, and $\mathcal{R}_o = \mathbb{F}_q[X_o]$. Then $\mathcal{R}_o$ is a principal ideal domain, and consequently Dedekind. If $\mathcal{K}$ is a finite separable extension of $\mathcal{K}_o$, then the integral closure of $\mathcal{R}_o$ in $\mathcal{K}$ is Dedekind. We say that $\mathcal{K}$ is A.F.F., (Algebraic Function Field).

$\mathcal{K}$ is a Global Field if $\mathcal{K}$ is either ANF or AFF.

(IV) Let $\mathcal{K}' = \mathcal{K}_o(X_1,\dots,X_n)$, X_i indeterminates and $\mathcal{P}$ prime ideal of $\mathcal{R}_o = \mathcal{K}_o[X_1,\dots,X_n]$. $\mathcal{R}_o$ is noetherian. Let $\mathcal{R} = \mathcal{R}_o/\mathfrak{p}$ and $\mathcal{K}$ its quotient field; suppose that the transcendent dimension of $\mathcal{K}$ over $\mathcal{K}_o$ is one. Let $\mathcal{V}$ be the variety of $\mathfrak{p}$ in $(\mathcal{K}^a)^n$ with $\mathcal{K}^a$ being the algebraic closure of $\mathcal{K}$. Then $\mathcal{V}$ is an affine curve having coordinate ring $\mathcal{R}$ and field of functions $\mathcal{K}$. We say that $\mathcal{V}$ is normal if $\mathcal{R}$ is integrally closed in $\mathcal{K}$. Consequently if $\mathcal{V}$ is normal, then $\mathcal{R}$ is Dedekind.

(V) Let $\{\mathfrak{p}_\alpha\}_{\alpha\in\Lambda}$ be a family of primes ideals of $\mathcal{R}$ and let $\mathcal{S} = (\cup\mathfrak{p}_\alpha)^c$; $\mathcal{S}$ is multiplicative. Let $\mathcal{R}_\Lambda = \mathcal{S}^{-1}\mathcal{R}$. If $\mathcal{R}$ is Dedekind then $\mathcal{S}^{-1}\mathcal{R}$ is also Dedekind and its integral closure in $\mathcal{L}$, $[\mathcal{L}:\mathcal{K}] =$ = finite, $\mathcal{K}$ quotient field of $\mathcal{R}$, coincides with $\mathcal{S}^{-1}\mathcal{S}$, $\mathcal{S}$ integral closure of $\mathcal{R}$ in $\mathcal{L}$. (see Lang, ANT., Algebraic Number Theory).

In particular if $\mathcal{B}$ is an ideal of $\mathcal{R}$ and $\{\mathfrak{p}_\alpha\}$ is the family of all prime divisors of $\mathcal{B}$ then we shall write $\mathcal{R} = \mathcal{R}_{\mathcal{B}}$. If $\mathcal{B} = (b)$ we simply write $\mathcal{R}_b$. Here we set $\mathcal{S}^{-1}\mathcal{S} = \mathcal{S}_{\mathcal{B}}$ or $\mathcal{S}_b$ respectively.

1.2. IDEALS OF A DEDEKIND DOMAIN.

If $\mathcal{A}$ is an $\mathcal{R}$-fractional ideal we say that $\mathcal{A}$ is an ideal of $\mathcal{K}$.

LEMMA 1. If $\mathcal{A}$ is an ideal of $\mathcal{K}$ then $\mathcal{A}$ is generated by at most two elements.

PROOF. If $\mathcal{A} = (a)$, done. If not, we can find $c \in \mathcal{R}$ such that $\mathcal{A}' = c\mathcal{A} \subset \mathcal{R}$. We fix $a \in \mathcal{A}'$ and then $\mathcal{R}/(a) = \oplus\{\mathcal{R}/\mathfrak{p}_i^{\alpha_i} \mid a = \prod \mathfrak{p}_i^{\alpha_i}\}$. $\mathcal{R}/\mathfrak{p}^\alpha$ is local artinian with only prime ideals (π^j), $j < \alpha$, $\mathfrak{p} = (\pi)$. Now, $\mathcal{A}' \bmod \mathfrak{p}_i^{\alpha_i} \subseteq (\pi_i^{\ell})$, for some $\ell = \ell(i)$. Now let $b \in \mathcal{R}$ with $\bar{b} = \pi_i^{\ell(i)}$ for all i. Now $\overline{\mathcal{A}'} = (\overline{a,b})$ whence $\mathcal{A}' = (a,b)$. Finally $\mathcal{A} = \frac{1}{c}\mathcal{A}' = (a/c, b/c)$. ∎

LEMMA 2. Let $\mathcal{A}$ and $\mathcal{B}$ be ideals of $\mathcal{K}$. We can choose $a_1, a_2, b_1, b_2 \in \mathcal{K}$ such that $\mathcal{A} = (a_1, a_2)$, $\mathcal{B} = (b_1, b_2)$ and $\mathcal{AB} = (a_1b_1, a_2b_2)$.

PROOF. We claim that we can choose basis for $\mathcal{A}$, $\mathcal{B}$ such that $v_\mathfrak{p}(a_1) = v_\mathfrak{p}(\mathcal{A})$ and $v_\mathfrak{p}(b_1) = v_\mathfrak{p}(\mathcal{B})$, for all $\mathfrak{p} \mid \mathcal{AB}$. For , we may assume $v_\mathfrak{p}(\mathcal{A}), v_\mathfrak{p}(\mathcal{B}) \geq 0$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_b$ be all the primes dividing $\mathcal{AB}$.

Let us for every j choose a basis for $\mathcal{A}$ such that $\mathcal{A} = (a_{1,j}, a_{2,j})$, $v_{\mathfrak{p}_j}(a_{1,j}) = v_{\mathfrak{p}_j}(\mathcal{A})$. By the chinese remainder theorem we choose $x_j \equiv 1 \bmod \mathfrak{p}_j^{\alpha(j)}$, $\alpha(j) = v_{\mathfrak{p}_j}(\mathcal{A})$ and $x_j \equiv 0 \bmod \mathfrak{p}_t^{\alpha(t)+1}$, $t \neq j$. Let $z = \Sigma x_j a_{1,j}$. Then $v_{\mathfrak{p}_j}(z) = v_{\mathfrak{p}_j}(a_{1,j})$ because $v_{\mathfrak{p}_j}(x_i, a_{1i}) \geq \alpha(j)+1$, if $i \neq j$. Repeat the argument for $\mathcal{B}$. Then, for all $\mathfrak{p} \mid \mathcal{AB}$ $v_\mathfrak{p}(a_1) = v_\mathfrak{p}(\mathcal{A})$ and $v_\mathfrak{p}(b_1) = v_\mathfrak{p}(\mathcal{B})$.
Now $v_\mathfrak{p}(a_1b_1, a_2b_2) = \min\{v_\mathfrak{p}(a_1, b_1), v_\mathfrak{p}(a_2b_2)\} = v_\mathfrak{p}(\mathcal{AB})$ since $v_\mathfrak{p}(a_1b_1) = v_\mathfrak{p}(a_1)v_\mathfrak{p}(b_1) = v_\mathfrak{p}(\mathcal{A})v_\mathfrak{p}(\mathcal{B}) = v_\mathfrak{p}(\mathcal{AB})$ and $v_\mathfrak{p}(a_2b_2) \geq v_\mathfrak{p}(\mathcal{AB})$. Hence $\mathcal{AB} = (a_1b_1, a_2b_2)$. ∎

PROBLEM OF THE INTEGRAL BASES:

To find a new adapted base for $\mathcal{L}_o$ and the elementary factors of $\mathcal{S}$ in $R[x]$.

1.3. LATTICES AND ORDERS (O'MEARA, PART IV, CHAPTER VIII).

Let $\mathcal{V}$ be a vector space over $\mathcal{K}$ and $\mathcal{L}$ be an $\mathcal{R}$-module in $\mathcal{V}$, say $\dim\mathcal{V} = n$. We say that $\mathcal{L}$ is a lattice in $\mathcal{V}$ in rank of $\mathcal{L}$ is n. We recall.

(1) There exists a base $\{x_1,\dots,x_n\}$ of $\mathcal{V}$ and fractionary ideals $\{\mathcal{A}_i\}$, such that $\mathcal{L} = \sum_{i=1}^{n} \mathcal{A}_i x_i$ with $\mathcal{A}_i | \mathcal{A}_{i+1}$. If $\mathcal{A}_i = \mathcal{R}$ for all i, we say that $\{x_i\}$ is an adapted base for $\mathcal{L}$.

(2) Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$, then $\mathcal{L}_1 \cap \mathcal{L}_2$ is a lattice such that as an abelian group is has finite index in both $\mathcal{L}_1$ and $\mathcal{L}_2$.

(3) Given two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ there exists a base for K such that $\mathcal{L}_1 = \Sigma\, a_i x_i$ and $\mathcal{L}_2 = \Sigma \mathcal{A}_i \tau_i x_i$ with $\tau_1 \supseteq \tau_2 \supseteq \dots \supseteq \tau_n$. The $\{\tau_i\}$ is uniquely determined in this way. They are called the *invariant factors* of $\mathcal{L}_2$ in $\mathcal{L}_1$. (τ_i are ideals of $\mathcal{R}$)

(4) If $\mathcal{V}_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of $\mathcal{V}$, $\mathfrak{p}$ prime of $\mathcal{R}$, and if $\mathcal{L}_{\mathfrak{p}}$ is the respective completion of $\mathcal{L}_{\mathfrak{p}}$, $\mathcal{L}_{\mathfrak{p}} \subset \mathcal{V}_{\mathfrak{p}}$, then $\mathcal{L}_{\mathfrak{p}}$ is an $\mathcal{R}_{\mathfrak{p}}$-lattice and $\mathcal{L} = \cap\, \{\mathcal{L}_{\mathfrak{p}} \cap \mathcal{V}\ ;\ \mathfrak{p} \text{ prime of } \mathcal{R}\}$.

Fixed a base $\{x_i\}$ for $\mathcal{V}$ such that $\mathcal{L} = \Sigma \mathcal{A}_i x_i$ then $\{x_i\}$ is adapted to $\mathcal{L}_{\mathfrak{p}}$ for almost all $\mathfrak{p}$.

DEFINITION. We say that a lattice $\mathcal{L}$ is an $\mathcal{R}$-order if its an $\mathcal{R}$-algebra. $\mathcal{L}$ is a maximal order if it is not properly contained in any other order. Given $\mathcal{L}$ then $\mathcal{L}_{\mathfrak{p}}$ is $\mathcal{R}_{\mathfrak{p}}$-maximal for almost all $\mathfrak{p}$. $\mathcal{L}$ is maximal iff $\mathcal{L}_{\mathfrak{p}}$ is maximal for all $\mathfrak{p}$.

REM. As $\mathcal{L} \sim \mathcal{K}^n$ we set $\mathcal{L} = \mathcal{V}$ and $\mathcal{L} = \mathcal{S}$. We fix a base for $\mathcal{L}$, namely $\{1,x,\dots,x^{n-1}\}$ and set $\mathcal{L}_o = \mathcal{R}[x]$. If $\mathcal{K}$ is global, then $\mathcal{S}$ in (Examples II and III) is unique maximal order of $\mathcal{L}$.

1.4. DISCRIMINANT

Let $y \in S$ and let E_o^* be the splitting field of f over K with $G = \mathrm{Gal}(E_o^*/K) = \{\sigma_o = \mathrm{id}, \sigma_1, \dots, \sigma_{n-1}\}$. We set $\Delta(y) = [\det(\sigma_i y^j)]^2$ and $D(y) = \prod_{i=1}^{n} (y - \sigma y) = f_i'(y)$ with $f_1(X) = \prod_{\sigma \in G} (X - \sigma y) = \prod_{j=1}^{n} b_j X^{n-j}$.

LEMMA 1. $\Delta(y) = (-1)^{n(n-1)/2} N_{E|K}(D(y)) = (-1)^{n(n+1)/2} b_n$.

PROOF. Lang, A.N.T., III, §3, Prop. 15. ∎

Let $W = \langle w_1, \dots, w_n \rangle_R$ =: the free R-module generated by the base $w_1, \dots, w_n$ of L/K. We set $DW = [\det(\sigma_i w_j)]^2 \neq 0$. If W is not free we define the discriminant DW as the g.c.d. of all DW_o with $W_o \subset W$ and W_o free R-module. We set $D(S) =: D(S/K)$ and if K is global $D(L/K) =: D(S/K)$.

REM 2. If $W_1 \subset W$, $W_1 = XW$, $X \in M_n(R)$, W_1, W free R-modules, then $DW_1 = (\det X)^2 DW$. If $W_1 = W$, then $\det X \in R^*$ =: units of R. ∎

REM 3. If S is a multiplicative set, then $S^{-1}D(B) = DS^{-1}(B)$ for any B either ideal of L or R-module containing $R[x]$. Also $S^{-1}DW = DS^{-1}W$ for any R-module $W \in L$. ∎

PROP 4. (Lang, ANF, III, §3, Prop. 10). If $M_1 \subset M_2$ are free R-modules of rank n, both contained in L, then

(1) $DM_1 | DM_2$

(2) $DM_1 = (DM_2)u$, $u \in R^* \Longrightarrow M_1 = M_2$. ∎

COR 5. If $W_1 \subset W_2$ are R-modules of rank n, then $DW_1 = (DW_2)I^2$. ∎

REM 6. If $\mathcal{W}_1 \subset \mathcal{W}_2$ and $(\mathcal{W}_1)_{\mathfrak{p}} = (\mathcal{W}_2)_{\mathfrak{p}}$ for all localization at primes $\mathfrak{p}$ of $\mathcal{R} \Longrightarrow \mathcal{W}_1 = \mathcal{W}_2$. Consequently if $D\mathcal{W}_1 = (D\mathcal{W}_2)u$, $u \in \mathcal{K}^*$, then $\mathcal{W}_1 = \mathcal{W}_2$.

(to see this we use Prop. 4 if $\mathcal{W}_i$ are free. If not we localize and apply the first part). $\blacksquare$

PROOF OF COR 5. We localize at $\mathfrak{p}$. Then $\mathcal{W}_1$ and $\mathcal{W}_2$ are free and $(D\mathcal{W}_1)_{\mathfrak{p}} = (D\mathcal{W}_2)_{\mathfrak{p}}\mathcal{I}^2_{\mathfrak{p}}$. Let $\mathcal{I} = \Pi\mathcal{I}^2_{\mathfrak{p}}$. Then $(D\mathcal{W}_1) = (D\mathcal{W}_2)\mathcal{I}^2$ because this holds at all $\mathfrak{p}$'s. $\blacksquare$

COR 7. Let $\mathcal{R}[x] \subset \mathcal{W} \subset \mathcal{S} \Longrightarrow D\mathcal{S} \mid D\mathcal{W}$, $D\mathcal{W} \mid \Delta(x)$ and $\Delta(x) = (D\mathcal{W})\mathcal{I}_o^2 = (D\mathcal{S})\mathcal{I}^2$. Consequently if $D\mathcal{W}$ (resp. $\Delta(x)$) is square free, then $D\mathcal{W} = D\mathcal{S}$ and $\mathcal{W} = \mathcal{S}$ (resp. $\Delta(x) = D\mathcal{S}$) and $R[x] = \mathcal{S}$. $\blacksquare$

COR 8. (Lang, ANT, II, §3, Prop. 16). If $p \nmid \Delta(x)/D\mathcal{S} \Longrightarrow \mathcal{S}_{\mathfrak{p}} = \mathcal{R}_{\mathfrak{p}}[x]$. $\blacksquare$

Let next $w \in \mathcal{S} \setminus \mathcal{R}[x]$, say $w = (\Sigma\ \lambda(i)x^i)d^{-1} = zd^{-1}$.

Set $\mathcal{I}' = \text{g.c.d.}(d, \text{g.c.d.}(\lambda(0),\dots,\lambda(n-1))$ and $d \sim \mathcal{I}\mathcal{I}'$.

LEMMA 9. $\mathcal{I}^2 \mid \Delta(x)$. If $\Delta(x)$ is square free then $\Delta(x) = D\mathcal{S}$ an $\mathcal{S} = \mathcal{R}[x]$.

PROOF. We consider the free module $\mathcal{W}_o$ generated by $(1, x, \dots, \hat{x}^j, \dots, x^{n-1}, w)$ (here $\hat{x}$ means omit x). We localize at $\mathfrak{p} \mid \mathcal{I}$. As $\mathcal{I}_{\mathfrak{p}} = (\pi^a)$ we get $D\mathcal{W}_o = \left(\frac{\lambda(j)}{d}\right)^2 \Delta(x)$. (Use elementary operations in the columns of $(\sigma_i w_j)$). We choose j such that if $\mathfrak{p} \mid \mathcal{I}$ then $\mathfrak{p} \nmid \lambda(j)$. Then at $\mathfrak{p}$, $\lambda(j)$ is a unit and as $D\mathcal{W}_o \in \mathcal{R}$ $\Longrightarrow \Pi^{2a} \mid \Delta(x)$ in $\mathcal{R}_{\mathfrak{p}}$ or $\mathfrak{p}^{2a} \mid \Delta(x)$, $a = v_{\mathfrak{p}}(\mathcal{I})$. This holds for all $\mathfrak{p} \mid \mathcal{I}$. Consequently $\mathcal{I}^2 \mid \Delta(x)$. $\blacksquare$

Closing this paragraph we shall prove:

LEMMA 10. Let $\mathcal{L} = \Sigma\, \mathcal{A}_i z_i \subset \mathcal{S}$, with $\{z_i\}$ being an adapted base for $\mathcal{R}[x] \subset \mathcal{L}$. Then $D\mathcal{L} = (\mathcal{A}_1,\dots,\mathcal{A}_n)^2 \Delta(x)$.

PROOF. By hypotheses $\mathcal{R}[x] \subset \mathcal{L}$ and this implies $x^j \in \mathcal{L}$ for all $0 \leq j \leq n-1$, hence $1 \in A_i$ for all i and consequently $b = \mathcal{A}_i^{-1} \supset$ $\supset \mathcal{R}$. Now $\mathcal{A}_i = (a_i, b_i)$ chosen such that $\pi A_i = (a_i, b_i)$. We consider the $\mathcal{R}$-modules $\mathcal{W}_1 = \langle \mathcal{A}_1 z_1, \dots, \mathcal{A}_n z_n \rangle$ and $\mathcal{W}_2 = \langle b_1 z_1, \dots, b_n z_n \rangle$.

Then $D\mathcal{W}_1 = (\pi \mathcal{A}_i)^2 D\langle z_1,\dots,z_n\rangle$ and $D\mathcal{W}_2 = (\pi b_i)^2 D\langle z_1,\dots,z_n\rangle$.

As $z_i \in \mathcal{R}[x]$. Then $\langle z_1,\dots,z_n\rangle = T_o\langle 1,x,\dots,x^{n-1}\rangle$ or

$D\langle z_1,\dots,z_n\rangle = (\det T_o^2)\Delta(x)$. Since $\{z_i\}$ is adapted $\ell_o = \det T$ is a unit modulo Δ.

Consequently the g.c.d. $(D\mathcal{W}_1, D\mathcal{W}_2, \Delta) = ((\pi a_i)^2, (\pi b_i)^2) =$ $= (\mathcal{A}_1,\dots,\mathcal{A}_n)^2 \Delta$ divides $D\mathcal{L}$. Now in order to prove the equality if suffices to localize our argument at all the primes dividing $\pi \mathcal{A}_i$.

1.5. TRACES

We shall denote by $t_i = Tr(L/K)(x^i)$, $i \geq 0$.

LEMMA 1. (Newton's Equations). Let $f(X) = X^n + \sum_{i=1}^{n} a_i X^{n-i}$, $a_i \in R$. Then the t_i satisfy the following equations

$$\begin{cases} i a_i + \sum_{j=0}^{i-1} a_j t_{i-j} = 0 \quad , \quad i=1,\ldots,n-1 \\ \\ \sum_{j=0}^{n} a_j t_{i-j} = 0 \quad , \quad i \geq n . \end{cases}$$

LEMMA 2. Let $T = (t_{ij})$, $t_{ij} = t_{i+j}$, $0 \leq i,j \leq n-1$. Then $\det T = \Delta(x)$.

Pf : For let $V = (\sigma_i x^j)$. Now $\Delta(x) = (\det V)^2 = \det {}^tVV$. Now ${}^tVV = (v_{ij})$, $v_{j\ell} = \sum_{i=1}^{n} \sigma_i x^j \sigma_i x^\ell = \Sigma\, \sigma_i (x^{j+\ell}) = t_{j+\ell}$ $\therefore$ ${}^tVV = T$. ∎

§2. GENERAL RESULTS

2.1. TRACE CONGRUENCES

We shall start with a trivial necessary condition to $w = z/d \in S \setminus R[x]$.

LEMMA 1. Let $w = z/d$, $z = \Sigma \lambda_i x^i$ and $\mathfrak{I}' = \text{g.c.d.}(d, \text{g.c.d.}(\lambda_o, \dots, \lambda_{n-1}))$, $d \sim \mathfrak{I}\mathfrak{I}'$. Then

$$(1) \qquad \sum_{i=0}^{n-1} \lambda_i t_{i+j} \equiv 0 \bmod \mathfrak{I}, \; 0 \le j \le n-1 .$$

We call the system (1) *Trace Congruences* and if we regard $\{\lambda_i\}$ as unknowns, then its determinant is T.

PROOF. As $z \in dR[x]$ we have that $\mathrm{Tr}(z) = (\Sigma \lambda_i t_i)/d$ or $\Sigma \lambda_i t_i \equiv 0 \bmod d$ and as $\mathfrak{I} | d$ we have $\Sigma \lambda_i t_i \equiv 0 \bmod \mathfrak{I}$. Now it suffices to repeat the argument for $x^j z$. ∎

Let T_{ij} = cofactor t_{ji}, and $\hat{T} = (T_{ij})$, $\therefore \hat{T}T = (\det t).\mathbb{1}$. $\mathbb{1}$ = identity matrix. We set for a fixed pair (m,j), $z = z(m) = \Sigma T_{mj} x^j$. Then

LEMMA 2. If $\lambda_j^* = T_{mj}$, $j = 0,\dots,n-1 \Longrightarrow (\lambda_j^*)$ satisfies the trace congruences mod Δ. Moreover $z^2 = \ell\Delta$ for some $\ell \in S$.

PROOF. The first part follows from $\hat{T}T = \Delta.\mathbb{1}$. Next we let $V=(v_{ij})$, $v_{ij} = \sigma_i x^j$, $0 \le i,j \le n-1$ and let $V' = (v'_{ij})$, $v'_{ij} = v_{ji}$ if $i \neq m$ and $v'_{mk} = \delta_{mk}$ = Kronecker's delta. Now if $T' = V'V = (\tau_{ij})$ we have, for $i \neq m$, $\tau_{ij} = \sum_{k=0}^{n-1} v'_{ik} v_{kj} = \Sigma v_{ki} v_{kj} = \Sigma \sigma_k x^{i+j} = t_{ij}$; For $i=m$, $\tau_{mj} = \Sigma \delta_{mk} v_{kj} = v_{mj} = \sigma_m x^j$. Hence T' differs from T only in $m^{\underline{th}}$ row. Now by expanding det T' by its $m^{\underline{th}}$ row we get

$$\det T' = \pm \sum_{j=1}^{n-1} (\sigma_m x^j) T_{mj} = \sigma_m (\Sigma\, x^j T_{mj}) = \sigma_m z\ .$$

Hence $z = \sigma_m^{-1} \det T' = \det(\sigma_m^{-1} T')$. Now $z^2 = (\det \sigma_m^{-1} T')^2 =$
$= \det(\sigma_m^{-1} T')^2 = \det [(\sigma_m^{-1} V')^2 (\sigma_m^{-1} V)^2] = [\det(\sigma_m^{-1} V)^2].\Delta(x)$.

As z^2 and $\Delta(x) \in S$, $\ell = \det(\sigma_m^{-1} V')^2 \in K$ and as ℓ is an integer in E_o^* ; we have consequently $\ell \in S$. ∎

§2.2. MAIN THEOREM

We say that the system (1) has rank $n-1$ mod Δ if there exists a pair (m,j) such that g.c.d. $(T_{mj},\Delta) = 1$. This implies that modulo any $\mathfrak{p}|\Delta$ the system has rank $n-1$.

THEOREM 1. Let the system (1) have hank $n-1$ mod Δ. Then

(a) $\mathcal{S} = \mathcal{R}[x]$ if $D\mathcal{S} = \Delta$ is square free as ideal of $\mathcal{R}$.

(b) If $\Delta \sim \mathcal{A}^2\mathcal{B}$, $\mathcal{A},\mathcal{B}$ ideals of $\mathcal{R}$, $\mathcal{B}$ square free. Then $\mathcal{S} = \mathcal{R} + \mathcal{R}x + \ldots + \mathcal{R}\hat{x}^j + \ldots + \mathcal{R}x^{n-1} + \mathcal{A}^{-1}z$ with $\{1,x,\ldots,\hat{x}^j,\ldots,x^{n-1},z\}$, being an adapted base for $\mathcal{R}[x]$. In this case $D\mathcal{S} = \mathcal{B}$.

PROOF. If Δ is square free. Then as $\Delta = (D\mathcal{S})\mathcal{I}^2 \Longrightarrow \Delta = D\mathcal{S}$ and by §1.4. $\mathcal{S} = \mathcal{R}[x]$.

Conversely assume that the system (1) has hank $n-1$. Then some $z = z(m) \not\equiv 0$ mod Δ. Also $\mathcal{A}^{-1}z \subset \mathcal{S}$. For if $\alpha \in \mathcal{A}^{-1}$, then $(\alpha z)^2 = \alpha^2 z^2 = \alpha^2 \ell\Delta(x)$. As $\alpha^2\Delta \subset \mathcal{R}$, $\alpha^2 z^2 \in \mathcal{S} \therefore \alpha z \in \mathcal{S}$.

Next we claim that $x^j \in \mathcal{S}_o = \langle 1,x,\ldots,\hat{x}^j,\ldots,x^{n-1},z\rangle$. For $T_{mj}x^j = z - \sum_{i\neq j} T_{mi}x^i \in \mathcal{S}_o$ and as $\mathcal{S}_o$ is a lattice (for $\mathcal{S}_o$ generates K) and as $\mathcal{S}_o \cap \mathcal{R}[x]$ is finite index in $\mathcal{S}_o$ we have that $\Delta^t x^j \in \mathcal{S}_o$ for some $t \geq 1$. From $(\Delta^t, T_{mj}) = 1$ we get that $x^j \in \mathcal{S}_o$. Now from 1.4, $D\mathcal{S}_o = \mathcal{A}^2\Delta = \mathcal{B}$.

Finally as $\mathcal{S} \supset \mathcal{S}_o \supset \mathcal{R}[x]$, $\Delta = (D\mathcal{S})\mathcal{I}^2 = (D\mathcal{S}_o)\mathcal{A}^2$, and $D\mathcal{S}_o = (D\mathcal{S})\mathcal{I}_o^2 = \mathcal{B}$ we have $\mathcal{I}_o^2 = (1)$, hence $D\mathcal{S} = \mathcal{B}$ again by §1.4 $\mathcal{S} = \mathcal{S}_o$. ∎

COROLLARY. If $\Delta = \mathcal{I}\mathcal{J}$ and g.c.d. $(T_{mj},\mathcal{I}) = 1$, then our theorem applies for $\mathcal{R}_{\mathcal{I}}$ and $\mathcal{S}_{\mathcal{I}}$.

§2.3. UNRAMIFIED EXTENSIONS

We let $y \in \mathbb{K}^a$ = algebraic closure of $\mathbb{K}$, be such that $y^2 = \eta\Delta$, η unit of $\mathbb{R}$. Let $\mathbb{E} = \mathbb{K}(y)$, $\mathbb{L}' = \mathbb{L}(y)$ and $\mathbb{E}^*$ be the splitting field of f over $\mathbb{E}$.

THEOREM 1. (c) Let $\mathbb{K}$ be global. If moreover f remains irreducible over $\mathbb{E}$, then both $\mathbb{L}'$ and $\mathbb{E}^*$ are unramified over $\mathbb{E}$.

PROOF. By part (b), $D(\mathbb{L}'/\mathbb{E})$ is a unit since z/y is an integer. Hence $\mathbb{L}'$ is unramified over $\mathbb{E}$. Now $\mathbb{E}^*$ is the composition of $(\mathbb{L}')^\sigma$, $\sigma \in Gal(\mathbb{E}^*/\mathbb{E})$, hence it is unramified over $\mathbb{E}$. ∎

As for the irreducibility of f over $\mathbb{E}$ we have the following simple criterion.

LEMMA 2. Let $f \in \mathbb{R}[x]$, $d^o f = n$ = odd, f irreducible over $\mathbb{K}$. Then f is irreducible over $\mathbb{E}$.

PROOF. Let $f = gh$ in $\mathbb{E}[X]$ with g irreducible and let $\alpha \in \mathbb{K}^a$ such that $g(\alpha) = f(\alpha) = 0$. If $d^o g = m$, $[\mathbb{E}(\alpha) : \mathbb{E}] = m$, $[\mathbb{E}:\mathbb{K}] = 2$ $\Longrightarrow$ $[\mathbb{E}(\alpha):\mathbb{K}] = 2m$ and as $\mathbb{E}(\alpha) = \mathbb{K}(\alpha,y) \subset \mathbb{K}(\alpha)$; $[\mathbb{K}(\alpha):\mathbb{K}] = n \Longrightarrow$ $n \mid 2m$. As $(m,2) = 1 \Longrightarrow n \mid m \Longrightarrow n = m$ and h is a constant. ∎

§2.4. INTEGRAL BASES: LOCALIZATION

If $w \in S$ then w is integer over $\mathcal{R}$ and a fortiori integral over $\mathcal{R}_{\mathfrak{p}}$ for all primes of $\mathcal{R}$. Hence $w \in S_{\mathfrak{p}}$. The converse is also valid in the following sense.

<u>LEMMA</u>. If $w \in S_{\mathfrak{p}}$, $w \notin \mathcal{R}_{\mathfrak{p}}[x]$, then there exists $\alpha \in S$, unit in $S_{\mathfrak{p}}$ s.t. $w \in S \setminus \mathcal{R}[x]$.

<u>PROOF</u>. Let $a_i \in \mathcal{R}_{\mathfrak{p}}$ such that $w^n + \Sigma\, a_i w^i = 0$, i.e. $v_{\mathfrak{p}}(a_i) \geq 0$ and let $a_i = a_i'/b_i, \ldots, v_{\mathfrak{p}}(b_i) \geq 0$. We write $b_i \sim \mathfrak{p}^{\alpha_i} \beta_i$ with $\mathfrak{p} \nmid \beta_i$. Let h be the order of C and let $\alpha \sim (\pi \mathcal{B}_i)$. Then $\mathfrak{p} \nmid \alpha$, and $\alpha \in \mathcal{R}$. Now if $z = \alpha w$, $z^n + \Sigma\, a_i \alpha^{n-i} z^i = 0$ and $a_i \alpha^{n-1} \sim a_i' \mathfrak{p}^{-\alpha_i} \mathcal{B}_i^{-1} \mathcal{B}_i^{c(n-i)} (\ldots) \subset \mathcal{R}$ because $v_{\mathfrak{p}}(a_j') \geq v_{\mathfrak{p}}(b_i) = \alpha_i$, and consequently all the exponents of the primes dividing $a_o \alpha^{n-1}$ are positive.

Finally as α is a $\mathfrak{p}$-unit, $w \notin \mathcal{R}[x]$. ∎

THE EQUATION $f(X) = X^n - aX^k - b = 0$

3.1. IRREDUCIBILITY OF $f(X) = X^n - aX^k - b$.

We shall state a few simple criterions for the irreducibility of f in $\mathcal{R}[X]$.

LEMMA 1. Let $f \in \mathcal{R}[X]$ be a monic polynomial

(a) If for some prime $\mathfrak{p}$ in $\mathcal{R}$, f is irreducible mod $\mathfrak{p}$, then f is irreducible.

(b) Assume that for some $\mathfrak{p}$ prime in $\mathcal{R}$, $f \equiv gh \bmod \mathfrak{p}$, $d^o g = 1$, and h irreducible mod $\mathfrak{p}$. If f is reducible in $\mathcal{R}[X]$, then f has a root in $\mathcal{R}$.

PROOF. Just observe that if f is reducible then it is reducible mod $\mathfrak{p}$ for all primes $\mathfrak{p}$ of $\mathcal{R}$. ∎

LEMMA 2. (CAPELLI) (Lang, Algebra, p.221). Let $\mathcal{K}$ be a field, and $f(X) = X^n - a$, $a \in \mathcal{K}$. Then f is reducible iff either

(a) a is an $m^{\underline{th}}$ power in $\mathcal{K}$, $m|n$

or

(b) $4|n$ and $a = -4c^4$ for some $c \in \mathcal{K}$. ∎

LEMMA 3. (EINSENSTEIN). Let $f \in \mathcal{R}[X]$ be a monic polynomial. If for some $\mathfrak{p}$ prime in $\mathcal{R}$, $f \equiv X^n \bmod \mathfrak{p}$ and $\mathfrak{p}^2 \nmid f(0)$, then f is irreducible.

Let us next look at the irreducibility of $X^n - a \bmod p$, for p prime in $\mathbb{Z}$, and $a \in \mathbb{Z}$. Let d be a generator of $F_p^* =$ the multiplicative group of the finite field with p elements.

LEMMA 4. Let g.c.d. $(n, (p-1)^t) = n$ for some $t \geq 1$. Then $f(X) = X^n - a$ is irreducible iff $a \equiv d^r \bmod p$ with g.c.d. $(n,r) = 1$.

PROOF. In fact if $(r,n) = m > 1$, $r = mu$, $n = mv$. Then $X^{mv} - d^{mu}$ is reducible. Conversely if $X^n - d^t$ is reducible then by Capelli's

Theorem $d^t = d_1^o$ for some $s|n$, $s > 1$. Now $d_1 \equiv d^r$ mod p, hence $d^t \equiv d^{rs}$ mod p or $t \equiv sr$ mod p-1. From $s|n$ we set that g.c.d. $(s,p-1) = s' > 1$ and $s'|t$. Consequently $(t,n) > 1$. ∎

COR 1. Let $f = X^n - aX^k - b \in \mathbb{Z}[X]$. Then f is irreducible if

(a) For some $p|a$, $b \equiv d^r$ mod p, g.c.d. $(n,r) = 1$ and g.c.d. $(n,r) = 1$ and g.c.d.$(n,p-1)^t) = n$ for some $t > 0$.

(b) For some $p|b$, $k=1$, $n = m+1$, $a \equiv d^r$, g.c.d. $(m,r) = 1$ and g.c.d. $(n,(p-1)^t) = m$ for some $t > 0$, and f has no root in $\mathbb{Z}$. ∎

COR 2. If $n = p^\ell$, p-prime in $\mathcal{R}$, b unit of $\mathcal{R}$ and $p^\ell \| a$. Then $f(X) = X^n - aX^k - b$ is irreducible if $p^2 \nmid f(b)$.

PROOF. Expand f at $x = b$ and set $y = x - b$. Then $f(y) = y^n + p \sum a_i' y^{n-1'} + f(b)$. Now $b^{p^s} \equiv b$ mod p hence $p|f(b)$ and by hypotheses $p^2 \nmid f(b)$. Consequently f is irreducible by Eisenstein. ∎

REM. $f(X) = X^p - aX - b$, $a \equiv 1$ mod p, $p \nmid b$ is irreducible.

Pf: reduce f mod p and observe that if x is a root of f mod p , then $x + c$ is also a root mod p for all c. ∎

EXAMPLE. $f(X) = X^n + aX^k + b$, a,b odd, is irreducible in the following situations,

$k = 1$, $n = 2,3,4,5,6,7,9,15,22,28,30,46,60$

$k = 2$, $n = 5,11,21,29,35$; $k = 4$, $n = 9, 15, 39, 57$.

$k = 3$, $n = 6,7,10,12,17,18,20,25,28,31,41,52$

$k = 5$, $n = 12,14,17,20,23,44,47$.

We obtain this table by reducing f mod 2 and look at Zierler and Brillhart. On primitive trinomials mod 2. (Inf and Control, v. 13, 1968, p. 541-554).

3.2. DISCRIMINANT OF $f(X) = X^n - aX^k - b$, AND TRACES

We recall that $\Delta(x) = (-1)^{\frac{n(n-1)}{2}} N(f'(x))$.

LEMMA 1. Let g.c.d. $(n-k,k) =$ g.c.d. $(n,k) = 1$. Then $\Delta(x) =$ $= (-1)^{\varepsilon} b^{k-1} \Delta_o$, $\Delta_o = k^k(n-k)^{n-k}a^n - (-b)^{n-k}n^n$ and $\varepsilon = \frac{n(n+1)}{2} +$ $+ nk+1$.

PROOF. We have $f'(X) = nX^{n-1} - akX^{k-1} = X^{k-1}(nX^{n-k} - ak)$. Let $z = nx^{n-k} - ak$. Let us find $N(z)$. We have $x^k(x^{n-k} - a) = b$ or $(x^{n-k})^k(x^{n-k} - a)^{n-k} = b^{n-k}$ or $(nx^{n-k})^k[nx^{n-k} - an]^{n-k} = n^n b^{n-k}$ or $(z+ak)^k[z+ak-an]^{n-k} = n^n b^{n-k}$ and
$N(z) = (-1)^n (ak)^k\{(ak-an)^{n-k} - n^n b^{n-k}\} =$
$= (-1)^{2n-k}\{k^k(n-k)^{n-k}a^n - n^n(-b)^{n-k}\} = (-1)^k \Delta_o$.
Now $N(f'(x)) = N(x)^{k-1}N(z) = (-1)^{n(k-1)}(-b)^{k-1}(-1)^k\Delta_o =$
$= (-1)^{nk+n+1} b^{k-1} \Delta_o$. Consequently $\Delta(x) = (-1)^{\varepsilon} b^{k-1}\Delta_o$ with
$\varepsilon = \frac{(n-1)n}{2} + kn + n = \frac{n(n+1)}{2} + kn+1$. ∎

REMARK. If $n = 2m$ is even, then $\varepsilon = m+1$

If $n = 2m+1$ is odd, then $\varepsilon = m$ for k even and $\varepsilon = m+1$ for k odd.

Let us now compute $\Delta(y)$ with $y = b/x$. Now
$\Delta(y) = (-1)^{\varepsilon'} N(F'(y)) = (-1)^{\varepsilon''} N[\frac{d}{dX}(-b^{n-1}X^{-n}f(X))\frac{dX}{dY}]_{X=x} =$
$= \pm N(-b^n x^{n-2} f'(x)) = \pm b^{n^2} N(x)^{-n-2} N(f'(x)) =$
$= \pm b^{n^2-n-2} \Delta(x) = \pm b^{\delta}\Delta_o$, with $\delta = n^2 - n-3+k$.

We recall that the minimal polynomial of y is
$F(Y) = Y^n + ab^{k-1} Y^{n-k} - b^{n-1}$.

Next we shall calculate the traces t_i. We first observe that the highest j such that t_j appears in T is $j=2n-2$. We shall assume $n > 2k$.

LEMMA 2: Let $n > 2k$. Then the only now zero traces appearing in T are

$$t_o = n \quad , \quad t_{n-k} = (n-k)a \quad , \quad t_n = nb$$

$$t_{2n-k} = (2n-k)ab \quad (\text{if } \ k > 1)$$

$$t_{2n-2k} = (n-k)a^2 \ , \text{ and } \ t_{3n-3k} = (n-k)a^3$$

in the case where $n < 3k-1$.

PROOF. In our case $a_o = 1$, $a_{n-k} = -a$ and $a_n = -b$. Let us apply Newton's equations: $t_o = n$ and $a_i = 0$, $0 < i < n-k$, hence $ia_i + a_o t_i + \ldots + a_{n-1}t_1 = 0$, $a_o t_i = 0$, $0 < i < n-k$ and $(n-k)a_k + a_o t_{n-k} + \ldots = (n-k)a_k + a_o t_{n-k} = 0$ or $t_{n-k} = (n-k)a$. Next if $n-k < i < n$, then $ia_i + a_o t_i + \ldots + a_{n-k}t_{i-(n-k)} + {}$ $+ a_{i-(n-k)}t_{n-k} + \ldots + a_{i-1}t_o = 0$. Since $i-(n-k) \neq n-k$ and $\neq$ zero because $i-(n-k) \geq n-k \Longrightarrow i \geq 2n-2k = n+(n-2k) \geq n \Longrightarrow t_{i-(n-k)} = 0$ similarly $a_{i-(n-k)} = 0$. Hence $ia_i = 0$ and $a_o t_i = 0$. Next we have from the second group of equations $t_{n+1} - at_{i+k} - bt_i = 0$, $0 \leq i \leq n-2$. For $i=0$, $t_n - at_k - bn = 0$ or $t_n = bn$ $(n > 2k)$. If $0 < i < n-k$, $t_i = 0$ and $t_{i+k} = 0$ if $i+k \neq n-k$. If $i+k = n-k$, $0 = n-2k$ and $n+i' = n+(n-2k) = 2n-2k$. Hence $t_{2n-2k} - at_{n-k} -$ $- bt_{n-2k} = 0$. As $t_{n-2k} = 0$, we have $t_{2n-2k} = at_{n-k} = (n-k)a^2$. Next if $i=n-k$, $t_{2n-k} = at_n + bt_{n-k} = anb + (n-k)ba = (2n-k)ab$. Now we may have $3n-3k < 2n-1$ or $n < 3k-1$. Here $3n-2k, 3n-k \geq$ $\geq 2n-2$ because $n > 2k$. More generally if $i \geq 4$, $i > j \Longrightarrow$ $in-jk > 2n$. For $i > j \Longrightarrow in-jk \geq i(n-k)$. For $i(n-k) < 2n \Longrightarrow$ $n < ik/(i-2)$, $n > 2k \Longrightarrow \frac{ik}{i-2} > 2k$, $i > 2i - 4$ or $i < 4$. Now for $i=2n-3k$, $t_{3n-3k} = at_{2n-2k} + bt_{2n-3k}$. As $2n-3k < n$, $t_{2n-3k} =$ $= 0$ unless $2n-3k = n-k$ or $n = 2k$. Consequetly $t_{3n-2k} =$ $= a(n-k)a^2$. Finally if $n > 3k-1$, $i > n-k$, $t_i \neq 0$ only for $i=1$, $i=2n-k$ and $i=2n-2k$. For these values $t_{n+i} = t_{2n}, t_{3n-k}, t_{3n-2k}$. If $t_{i+k} \neq 0 \Longrightarrow i+k=n$, $2n-k$ or $2n-2k$, i.e. $i=n-k$, $3n-2k$, $3n-3k$ already studied. Hence for all the other's i, $t_{n+i} = 0$. ∎

COR. If $n=2k \Longrightarrow t_o = 2k$, $t_k = t_{n-k} = ka$, $t_{2k} = 2kb + a^2k$ and $t_{3k} = 3kab + a^3k$.

3.3. TRACE CONGRUENCES: Case $k=1$, $n \geq 3$

Let $\mathcal{I}$ be an ideal such that $\mathcal{I}^2 | \Delta$ and g.c.d. $(\mathcal{I}, n(n-k)kab)=1$. If g.c.d. $((n-k)na, nb) = 1$ and g.c.d. $(\mathcal{I}, b) = 1$; then g.c.d. $(\mathcal{I}, (n-k)nkab) = 1$. We shall we working modulo $\mathcal{I}$, and for any fixed $d \in \mathcal{R}$ we shall denote by $d^{-1} \in \mathcal{R}$ a fixed element of $\mathcal{R}$ such that $dd^{-1} \equiv 1$ modulo $\mathcal{I}^2$. All congruences unless otherwise stated are modulo $\mathcal{I}$. Now the congruences (1) becomes:

$$(2) \quad \begin{cases} \text{(I)} \ n\lambda_o + (n-k)a\lambda_{n-1} \equiv 0 \\ \text{(II)} \ nb\lambda_{n-j} + (n-k)a\lambda_{n-1-j} \equiv 0 \ , \ 1 \leq j \leq n-2 \\ \text{(III)} \ nb\lambda_1 + (n-1)a\lambda_o + (n-1)a^2\lambda_n \equiv 0 \quad (j=n-1). \end{cases}$$

PROOF. (I) is the first congruence: here $\Sigma \lambda_i t_{i+j} \equiv 0$, $j = 0$ and $i \in [0, n-1]$, $t_i \neq 0 \iff i=0, n-1$. Now for $1 \leq j \leq n-2$, $i + j \in [j, n-1+j]$ and here only $i+j=n, n-1$ yields $t_{i+j} \neq 0$. Finally for $j=n-1$ the indices lie in $[n-1, 2n-2]$ and only t_{n-1}, t_n and t_{2n-2} are $\neq 0$. ∎

LEMMA 1. (2) Has up to a multiplicative constant a unique solution.

PROOF. From (I) $\lambda_{n-1} = c\lambda_o$, $c = -n(n-1)^{-1}a^{-1}$, and by recurrence (II) $\lambda_{n-1-j} = (cb)^j\lambda_{n-1}$, $j=1,\dots,n-2$. (III)' yields $\lambda_1 = ab^{-1}n^{-1}\lambda_o$. Hence all λ_j's can be uniquely expressed in terms of λ_o. ∎

REM. If $a = na_o$ and $b = -b_o(n-1)$ with g.c.d. $(a_o b_o, \Delta) = 1$, Then $R = a_o b_o^{-1}$ is a double root of $f(X) = X^n - na_oX + (n-1)b_o$ modulo $\Delta_o = a_o^n - b_o^{n-1}$. If we set $\lambda_o = (n-1)\lambda_o'$, $\mathcal{J}$ = g.c.d. $(n(n-1), \Delta)$, $\Delta = \mathcal{I}\mathcal{J}$, then (2) become

$$\lambda_o' + a_o\lambda_{n-1} \equiv a\lambda_{n-1-j} - b_o\lambda_{n-j} \equiv 0 \bmod I .$$

and again

$$z = -(n-1)a_o^{n-1} + \sum_{j=1}^{n-1} b_o^{n-j-1} a_o^{j-1} x^j$$

and

$$z^2 = \Delta_o\{(n-1)^2 a_o^{n-2} - \sum_{t=2}^{n-1} (t-1) b_o^{n-t-1} a_o^{t-2} x^t\}$$

3.4. TRACE CONGRUENCES: CASE $n > 3k-1$

Here we have the following congruences:

$$(3)\begin{cases} \text{(I)}\ n\lambda_o + (n-k)a\lambda_{n-k} \equiv 0 \\ \text{(II)}\ nb\lambda_{n-j} + (n-k)a\lambda_{n-j-k} \equiv 0\ ,\ j=1,\dots,n-2k \\ \text{(III)}\ (n-k)a\lambda_{k-\ell} + nb\lambda_{2k-\ell} + (n-k)a^2\lambda_{n-\ell} \equiv 0 \quad \ell = 1,\dots,k \\ \text{(IV)}\ nb\lambda_{k-\ell} + (n-k)a^2\lambda_{n-k-\ell} + (2n-k)\lambda_{n-\ell} \equiv 0 \quad \ell = 1,\dots,k-1. \end{cases}$$

We recall that in $[0,2n-2]$ the only i's such that $t_i \neq 0$ are $0 < n-k < n < 2n-2k < 2n-k < 2n-2$.

PROOF. (I) Trivial. (II). For $j=1,\dots,n-2k$, we look at $\Sigma\ \lambda_i t_{i+j} = \Sigma\ \lambda_{s-j} t_s$ with $j \leq s \leq n+j-1$, because $0 \leq s-j \leq n-1$. In this interval we only have $s = n-k$, and n, with $t_s \neq 0$, i.e. $t_n\lambda_{n-j} + t_{n-k}\lambda_{n-k-j} \equiv 0$. Also $1 \leq j \leq n-2k < n-k \leq n+j-1 < n+n-2k = 2n-2k$.

(III) Next for $j \in [n-2k+1,n-k]$ we have that $n-2k < j \leq n-k < n < 2n-2k = n-2k+1 + n-1 \leq j+k-1 \leq n-k+n-1 = 2n-k-1$, and our equations become:

$$\lambda_{n-k-j}t_{n-k} + \lambda_{n-j}t_n + \lambda_{2n-2k-j}t_{2n-2k} \equiv 0\ .$$

We set $n-k-j = k-\ell$ or $\ell = -n+2k+j$ and as $j \in [n-2k+1, n-k] \Longrightarrow \ell \in [1,k]$; also $n-j = 2k-\ell$ and $2n-2k-j = k-\ell+n-k=n-\ell$. Now our equations become

$$(n-k)a\lambda_{k-\ell} + nb\lambda_{2k-\ell} + (n-k)a^2\lambda_{n-\ell} \equiv 0\quad ,\quad \ell = 1,\dots,k\ .$$

(IV) Now $j \in [n-k+1,n-1]$ and we have that $n-k < n-k+1 \leq j < n < 2n-2k < 2n-k = (n-k+1) + n-1 \leq n-1+j$ and our equations become:

$$\lambda_{n-j}t_n + \lambda_{2n-2k-j}t_{2n-2k} + \lambda_{2n-k-j}t_{2n-k} \equiv 0 \ .$$

We set $n-j = k-\ell$. Then $2n-2k-j = k-\ell+n-2k = n-k-\ell$ and $2n-k-j = k-\ell+n-k = n-\ell$. Hence

$$\lambda_{k-\ell}t_n + \lambda_{n-k-\ell}t_{2n-2k} + \lambda_{n-\ell}t_{2n-k} \equiv 0$$

or

$$nb\lambda_{k-\ell} + (n-k)a^2\lambda_{n-k-\ell} + (2n-k)ab\lambda_{n-\ell} \equiv 0 \ .$$

Finally if $j \in [n-k+1,n-1] \Longrightarrow \ell = k-n+j$ lies between $k-n+(n-k+1)$ and $k-n+(n-1)$ or $\ell \in [1,k-1]$ or $\ell = 1,\dots,k-1$.

<u>LEMMA</u> 1. If $n \geq 3k-1$, then up to a multiplicative constant, the trace congruences have a unique solution.

<u>PROOF</u>. We shall show that we can resolve (3) and find λ_j , $j=1,\dots,n-1$, in terms of λ_o . We claim that:

$$\text{(I)}' \quad \lambda_{n-k} \equiv -((n-k)a)^{-1}n\lambda_o =: M\lambda_o$$

$$\text{(II)}' \quad \lambda_{n-j} \equiv -(n-k)a(nb)^{-1}\lambda_{n-k-j} =: C\lambda_{n-k-j} \ ; \ j=1,2,\dots,n-2k$$

$$\text{(III)}' \quad \lambda_{2k-j} \equiv -k(n-k)a^2b^{-1}n^{-2}\lambda_{n-j} =: H\lambda_{n-j} \ , \ j=1,2,\dots,k$$

$$\text{(IV)}' \quad \lambda_{k-j} \equiv -(n-k)an^{-1}\lambda_{n-j} =: F\lambda_{n-j} \ , \ j=1,2,\dots,k-1 \ .$$

For (I)' and (II)' are immediate. Next if we replace (II)' in (IV) we get

$$nb\lambda_{k-j} + (n-k)a^2[-(n-k)^{-1}a^{-1}nb]\lambda_{n-j} + (2n-k)ab\lambda_{n-j} \equiv$$

$$nb\lambda_{k-j} + [-anb + (2n-k)ab]\lambda_{n-j} = nb\lambda_{k-j} + (n-k)ab\lambda_{n-j} \equiv 0$$

and we get (IV)'.

Next we replace those values in (III). We get $(n-k)a\lambda_{k-j} + nb\lambda_{2k-j} + (n-k)a^2\lambda_{n-j} \equiv \{(n-k)a[-(n-k)an^{-1}] + (n-k)a^2\}\lambda_{n-j} + nb\lambda_{2k-j} \equiv nb\lambda_{2k-j} + a^2(n-k)[-n^{-1}(n-k)+1]\lambda_{n-j} \equiv nb\lambda_{2k-j} + a^2(n-k)n^{-1}k\lambda_{n-j} \equiv 0$ or $\lambda_{2k-j} \equiv -a^2b^{-1}(n-k)kn^{-2}\lambda_{n-j}$.

We now iterate (II)' we get

$$\lambda_{n-j} = \lambda_{n-j-k} \equiv C^2\lambda_{n-j-2k} \equiv \ldots \equiv C^t\lambda_{n-j-tk}$$

We set $n = ks + m$. From $n-j-tk \geq k = n-(n-2k)$, $j = 1,\ldots,n-k$, we get $n-j-tk-k \geq 0$ or $(s-t-1)k + m-j \geq 0$. If $j \leq m$, then the highest value of t is $s-1$ and if $m < j \leq k$ the highest value is $s-2$. Then, for $j \leq m$, $\lambda_{n-j} \equiv C^{s-1}\lambda_{n-(s-1)k-j}$ and $n-sk+k-j = m+k-j$. For $j > m$, $\lambda_{n-j} \equiv C^{s-2}\lambda_{n(s-2)k-j}$ and $n-(s-2)k-j = m+2k-j$. Hence

$$\text{(II)"} \quad \lambda_{n-j} \equiv \begin{cases} C^{s-1}\lambda_{m+k-j}, & j \leq m \\ C^{s-2}\lambda_{m+2k-j}, & j > m \end{cases}$$

By replacing in (III)' $2k-\ell$ by $m+k-j$ and $2k+m-j$, (if respectively $j \leq m$ or $j > m$) we get

$$\text{(III)"} \quad \begin{cases} \lambda_{m+k-j} \equiv H\lambda_{n-j+m-k}, & j=1,\ldots,m \\ \lambda_{2k+m-j} \equiv H\lambda_{n+m-j}, & j=m+1,\ldots,k. \end{cases}$$

for $2k-\ell = m+k-j \iff n-\ell \equiv n+m-k-j$ and

$2k+m-j = 2k-\ell \iff n-\ell \equiv n+m-j$

$m-j = -\ell$.

Hence

$$\begin{cases} \lambda_{n-j} \equiv C^{s-1}H\lambda_{n-j+(m-k)} & , \ j=1,\dots,n \\ \lambda_{n-j} \equiv C^{s-2}H\lambda_{n-j+m} & , \ j=m+1,\dots,k \end{cases}$$

We define

$$\alpha(j) = \begin{cases} j-m & , \ j=m+1,\dots,k \\ j-m+k & , \ j=1,\dots,m \ , \text{ i.e., } \alpha(j) \equiv j-m \bmod k \end{cases}$$

and $\alpha(j)$ is then a permutation of $\{1,\dots,k\}$.

Let $nk - \nu m = 1$ (for $(n,k) = (m,k) = 1$), and set $\alpha^{(\ell)}(j) = \alpha(\alpha^{(\ell-1)}(j))$, $\alpha^{(0)}(j) = j$. Then, by induction $\alpha^{(\nu)}(j) \equiv j-\nu m \equiv j+1 \bmod k$. If we set $C^{s-2}H = W$ and $\varepsilon(j) = 1$ if $j=1,\dots,m$ and $\varepsilon(j) = 0$ otherwise. These $\alpha(j) = j-m+\varepsilon(j)k$ and

$$\lambda_{n-j} = C^{\varepsilon(j)} W \lambda_{n-\alpha(j)} = C^{\varepsilon(j)+\varepsilon(\alpha(j))} \cdot W^2 \lambda_{n-\alpha^{(2)}(j)} \equiv$$

$$\equiv C^{\varepsilon'} W^i \lambda_{n-\alpha^{(i)}(j)} \quad \text{where}$$

$\varepsilon' \equiv \Sigma\{\varepsilon(\alpha^{(\ell)}(j)) \mid \ell = 0,1,\dots,i-1\}$.

Now by iterating ν times and observing that $1 \le \alpha^{(\ell)}(j) \le k$ we must have $\lambda_{n-j} =: S\lambda_{n-j-1}$, with $S = S(j)$, $S = C^{\varepsilon} W^{\nu}$, $j = 1,\dots,k$, $\varepsilon = \sum_{\ell=0}^{\nu-1} \varepsilon(\alpha^{(\ell)}(j))$. Now, we claim that

$$\alpha^{(\nu)}(j) = j - \nu m + \sum_{i=0}^{\nu-1} \alpha^{(i)}(j)k \ , \ 1 \le j \le k \ .$$

For $\alpha(j) = j-m+\varepsilon(j)k$ and $\alpha(\alpha(j)) = j-m+\varepsilon(j)k + \varepsilon(\alpha(j))k-m = j-2m + (\varepsilon(j)+\varepsilon(\alpha(j)))k$. Now it suffices to apply induction. Next $\alpha^{(\nu)}(j) \equiv j-\nu m \quad j+1 \bmod k$ and $1 \le \alpha^{(\nu)}(j) \le k$. This implies for $j \leq k-1$, $1 \leq j+1+\alpha_o k \leq k$ or $\alpha_o = 0$. Hence $\alpha^{(v)}(j) = j+1$ and by the same argument $u = \sum_{i=1}^{v-1} \alpha^{(i)}(j)$. Now $S \equiv C^u W^v \equiv C^{u+sv-2v} H^v \equiv [-(n-k)b^{-1}]^{u+sv-v} [an^{-1}]^{u+sv} k^v$. We have

$$\lambda_{n-1} = S\lambda_{n-2} = S^j \lambda_{n-j-1} = S^{k-1}\lambda_{n-k} \quad , \quad i \leq j \leq k-1$$

By (I)' $\lambda_{n-k} = M\lambda_o$ and if we set $\lambda_{n-1} = S^{n-1}U\lambda_o$ we get $\lambda_{n-j} = S^{n-j}U\lambda_o$, $U = S^{(k-1)-(n-1)}M = S^{-(u-k)}M$. Now by (II)' we get $\lambda_{n-j-tk} = C^{-t}\lambda_{n-j}$, $j=1,\ldots,k$, with $t \leq s-1$, and the lowest index is k because the last equation $\lambda_{n-(n-sk)} = C\lambda_{n-k-(n-2k)}$ or $\lambda_{2k} = C\lambda_k$. Now in order to determine λ_ℓ, $\ell < k$, we use (IV)'. Consequently all the values are uniquely determined by λ_o and (I)', (II)', (III)' and (IV)'. ▪

3.5. TRACE CONGRUENCES: CASE $2k < n < 3k-1$

Here (I), (II) and (III) are the same, but (IV) ranges from $j=n-k+1$ to $2n-3k$, because $n-k-1 \leq n-k+j \leq 2n-3k < n < 2n-2k < 2n-k < 2n-3k + n-1 = 3n-3k-1$. We have

$$\text{(IV)}\quad nb\lambda_{k-\ell} + (n-k)a^2\lambda_{n-k-\ell} + (2n-k)ab\lambda_{n-\ell} \equiv 0$$

obtained from the $\Sigma\,\lambda_{i-j}\,t_j \equiv 0$ by replacing $n-j$ by $k-\ell$ and $1 \leq \ell \leq n-2k$.

For the last set of congruences j ranges from $2n-3k+1$ to $n-1$ and in each congruence $i \in [j, j+n-1]$ and here n, $2n-k$, $2n-2k$, $3n-3k \in [j, j+n-1]$. Hence

$$\text{(V)}\quad \lambda_{n-j}t_n + \lambda_{2n-k-j}t_{2n-k} + \lambda_{2n-2k-j}t_{2n-2k} + \lambda_{3n-3k-j} \equiv 0$$

or if $\ell = n-j$.

$$\text{(VI)}\quad nb\lambda_{\ell} + (2n-k)ab\lambda_{n-k+\ell} + (n-k)a^2\lambda_{n-2k+\ell} + (n-k)a^3\lambda_{2n-2k+\ell} \equiv 0$$

and $\ell = 1,\dots,n-(2n-3k+1) = 3k-n-1$.

Let us now prove that

LEMMA. If $2k < n < 3k-1$ then up to a multiplicative constant the congruences (I)-(V) have a unique solution.

We set $n=2k+m$, $k=tm+m_o$ and $\alpha = -t_{n-k}t_n^{-1}$, $\beta = -t_{2n-2k}t_n^{-1}$, $\gamma = -t_{2n-k}t_n^{-1}$ and $\delta = -t_{3n-3k}t_n^{-1}$. From (I) we have $\lambda_{n-k} =: M\lambda_o$, $M = -t_o t_{n-k}^{-1}$. (II) Yields: $\lambda_{n-j}t_n + \lambda_{n-j-k}t_{n-k} \equiv 0$ or $\alpha\lambda_{k+m-j} = \lambda_{2k+m-j}$, $j=1,\dots,n-2k = m$. Next we see that $n-k=k+m$, $2n-2k = 2k+2m$, $2n-k = 3k+2m$ and $3n-3k = 3m+3k$. Then (III) writes

$$\lambda_{n-j} \equiv \alpha\lambda_{n-k-j} + \beta\lambda_{2n-2k-j}\ ,\ j=m+1,\dots,m+k$$

or

$$\lambda_{2k-j} \equiv \alpha\lambda_{k-j} + \beta\lambda_{2k+m-j}\ ,\ j=1,\dots,k\ .$$

Next (IV) is $\lambda_{n-j}t_n + \lambda_{2n-2k-j}t_{2n-2k} + \lambda_{2n-k-j}t_{2n-k} \equiv 0$ or $\lambda_{n-j} \equiv \beta\lambda_{2n-2k-j} + \gamma\lambda_{2n-k-j}$ where j ranges from $n-k-1 = m+k+1$ to $2n-3k = k+2m$, or

$$\lambda_{2k+m-j} = \beta\lambda_{2k+2m-j} + \gamma\lambda_{3k+2m-j}\ .$$

Finally (V) gives

$$\Sigma\{\lambda_{r-j}t_r \mid r=n\ ,\ 2n-2k,\ 2n-k,\ 3n-3k\} \equiv 0$$

or

$$\lambda_{n-j} \equiv \beta\lambda_{2n-2k-j} + \gamma\lambda_{2n-k-j} + \delta\lambda_{3n-3k-j}$$

$$\lambda_{2k+m-j} = \beta\lambda_{3k+2m-j} + \gamma\lambda_{3k+2m-j} + \delta\lambda_{3m+3k-j}$$

j ranging from $2m-3k+1 = 2m+k+1$ to $n-1 = 2k+m-1$.

We next break the congruences (III) and (V) as follows:

$$(\mathrm{III})_\sigma \qquad \lambda_{2k-\sigma m-\ell} \equiv \alpha\lambda_{k-\sigma m-\ell} + \beta\lambda_{k-(\sigma-1)m-\ell}$$

here $\ell = j-m$, $\ell = 1,\dots,m$ if $\sigma < t$ and $\ell = 1,\dots,m_o-1$ if $\sigma = t$.

$$(\mathrm{V})_\sigma \quad \lambda_{k-\sigma m-\ell} \equiv \beta\lambda_{k-(\sigma-1)m-\ell} + \gamma\lambda_{2k-(\sigma-1)m-\ell} + \delta\lambda_{2k-(\sigma-2)m-\ell}$$

with $\ell = 1,\dots,m$ if $0 \leq \sigma \leq t-1$ and $\ell = 1,\dots,m_o-1$ if $\sigma = t$.

<u>LEMMA</u>. We can find $\Lambda(i,\sigma) \in \mathbb{R}$, $i=1,2$, independent of j, such that

$$\lambda_{2k-\sigma m-j} = \Lambda(2,\sigma)\lambda_{m+k-j}$$

$$\lambda_{k-\sigma m-j} = \Lambda(1,\sigma)\lambda_{m+k-j}$$

with $\sigma = -1,0,1,\dots,t$, $j=1,\dots,m$ if $\sigma \neq t$ and $j=1,\dots,m_o-1$ if $t = \sigma$.

<u>PROOF</u>. We proceed by induction on σ. For $\sigma = -1$ our system becomes

$$\lambda_{2k+m-j} = \Lambda(2,-1)\lambda_{m+k-j} \;,\; \Lambda(2,-1) = \alpha \quad \text{(by (II))}$$

$$\lambda_{k+m-j} = \Lambda(1,-1)\lambda_{m+k-j} \;,\; \Lambda(1,-1) = 1 \;.$$

For $\sigma = 0$ (IV) implies

$$\lambda_{k-j} = \beta\lambda_{k+m-j} + \gamma\lambda_{2k+m-j} = \Lambda(1,0)\lambda_{k+m-j}$$

with $\Lambda(1,0) = \beta + \gamma\alpha$. By (III)

$$\lambda_{2k-j} = \alpha\lambda_{k-j} + \beta\lambda_{2k+m-j} \equiv \Lambda(2,0)\lambda_{k+m-j}$$

with $\Lambda(2,0) = \alpha\Lambda(1,0) + \beta\alpha$.

Assume next that our formulas are valid for all $\sigma-\ell$, $\ell > 0$. From $(\text{V})_\sigma$ we get that

$$\lambda_{k-\sigma m-j} = [\beta\Lambda(1,\sigma-1) + \gamma\Lambda(2,\sigma-1) + \delta\Lambda(2,\sigma-2)]\lambda_{k+m-j} \;,$$

hence $\Lambda(1,\sigma) = \beta\Lambda(1,\sigma-1) + \gamma\Lambda(2,\sigma-1) + \delta\Lambda(2,\sigma-2)$ and by $(\text{III})_\sigma$ $\lambda_{2k-\sigma m-j} \equiv \Lambda(2,\sigma)\lambda_{k+m-j}$ where $\Lambda(2,\sigma) = \alpha\Lambda(1,\sigma) + \beta\Lambda(2,\sigma-1)$. ∎

We look now at

$$\begin{cases} \lambda_{2k-tm-j} = \Lambda(2,t)\lambda_{k+m-j}\ , & j=1,\dots,m_o \\ \lambda_{2k-(t-1)m-j} = \Lambda(2,t-1)\lambda_{k+m-j}\ , & j=m_o+1,\dots,m \end{cases}$$

We set

$$2k-tm-j = k+m_o-j = (k+m)-(m-m_o+j)$$

$$2k-(t-1)m-j = k+m+m_o-j = (k+m)-(j-m_o)$$

or

$$\lambda_{k+m-(m+j-m_o)} = \Lambda(2,t)\lambda_{k+m-j}\ , \quad i \le j \le m_o$$

$$\lambda_{k+m-(j-m_o)} = \Lambda(2,t-1)\lambda_{k+m-j}\ , \quad m_o+1 \le j \le m\ .$$

$$\therefore \quad \lambda_{k+m-j} = \Omega\lambda_{k+m-\alpha(j)}\ , \quad j=1,\dots,m$$

where

$$\alpha(j) = \begin{cases} j-m_o+m\ , & 1 \le j \le m_o \\ j-m_o\ , & m_o+1 \le j \le m \end{cases}$$

and $\Omega = \Lambda(2,t)$ or $\Lambda(2,t-1)$ according to $j \le m_o$ or not. Hence $\alpha(j)$ is a permutation of $\{1,\dots,m\}$ and $\alpha(j) \equiv j-m_o \bmod m$. By iteration $\alpha^{(\ell)}(j) =: \alpha(\alpha^{(\ell-1)}(j)) \equiv j-\ell m_o \bmod m$. Now g.c.d. (n,k) = g.c.d. $(m,k) = 1$ implies g.c.d. $(m,m_o) = 1$ or we can write $u'm - v'm_o = 1$ for some $u',v' \in \mathbb{Z}$. Consequently $\alpha^{(v')}(j) \equiv j-v'm_o \equiv j+1 \bmod m$. Hence $\alpha^{(v')}(j) = j+1$. By iteration $\lambda_{k+m-j} \equiv \Omega(v',j)\lambda_{k+m-j-1}$, with $\Omega(v',j) = \Lambda(2,t)^{\ell(1)}\Lambda(2,t-1)^{\ell(2)}$, $\ell(1) + \ell(2) = v'$. From $\lambda_{k+m} = \lambda_{n-k} = M\lambda_o = \Omega^{(0)}\lambda_{k+m-1} = \Omega^{(1)}\lambda_{k+m-2} = \dots = \Omega^{(m-1)}\lambda_{k-1}$, we get $\lambda_{k+m-j} = S(j)\lambda_o$, $0 \le j \le m-1$. Now (II) implies $\lambda_k = \alpha\lambda_o + \beta\lambda_{k+m} = S(k)\lambda_o$. From

$\lambda_{2k-\sigma m-j} = \Lambda(2,\sigma)S(j)\lambda_o$ and $\lambda_{k-\sigma m-j} = \Lambda(1,\sigma)S(j)\lambda_o$ we get that all λ_{2k-j} and λ_{k-j} are uniquely determined by λ_o, $j=1,\ldots,k-1$. Hence, by (IV) we can express all λ_{n-j} uniquely in terms of λ_o. This complete the proof of Lemma 1. ∎

3.6. THE ZEROS OF $f(X)$ MODULO $\mathcal{I}$, $\mathcal{I}$ DIVIDES Δ

We shall assume $n \geq 2k \geq 2$. We set

$$S = k^{v}[-(n-k)b^{-1}]^{u+sv-v}[an^{-1}]^{u+sv} \mod I$$

where $n = ks+m$, $ku - mv = 1$, $k > 1$. We take $s = 1 = u$, $v = 0$ if $k=1$.

LEMMA 1. S satisfies the following congruences modulo $\mathcal{I}$:

$$(c) \quad \begin{cases} S^{k} \equiv C \equiv -(n-k)b^{-1}an^{-1}, \quad S^{n} \equiv -(n-k)b^{-1}k^{-1} \\ S^{n-k} \equiv k^{-1}a^{-1}n . \end{cases}$$

PROOF. We recall that g.c.d. $(\mathcal{I}, n(n-k)kab) = 1$ and $\mathcal{I} \mid \Delta$. Hence

$$k^{k}(n-k)^{n-k}a^{n} \equiv (-b)^{n-k}n^{n} \mod \mathcal{I}$$

or

$$\rho =: k^{k}[-(n-k)b^{-1}]^{n-k}(an^{-1})^{n} \equiv 1 \mod \mathcal{I}.$$

Now

$$S^{k} = k^{kv}[-(n-k)b^{-1}]^{ku+ksv-kv}[an^{-1}]^{ku+ksv}$$

as

$$uk + ksv - kv = 1+mv + svk - vk = 1 + nv - vk = 1 + (n-k)v$$

and

$$uk + vsk = 1+mv + vsk + 1+nv \ ; \text{ hence}$$

$$S^{k} = \rho^{v}(an^{-1})(-(n-k)b^{-1}) = -(n-k)ab^{-1}n^{-1} \mod \mathcal{I}$$

Next

$$S^n = k^{kn}[-(n-k)b^{-1}]^{nu+nsv-vn}(an^{-1})^{(u+sv)n}$$

but

$$nv = ksv + mv = ksv + uk-1 = k(u+sv) - 1$$

$$(n-k)(u+sv) = nu-ku+usv = n(u+sv-v) - 1 .$$

hence

$$S^n = \sigma^{u+sv}k^{-1}(-(n-k)b^{-1} \equiv -k^{-1}b^{-1}(n-k)$$

and

$$S^{n-k} = S^n S^{-k} \equiv [-k^{-1}b^{-1}(n-k)][-(n-k)ab^{-1}n^{-1}]^{-1} \equiv k^{-1}a^{-1}n.$$

REM. If $n \geq 3k-1$ we also have $W^k \equiv C^{-m}$, $S^k \equiv C$ and $S^m \equiv W^{-1}$ where $W = C^{s-2}H$, $H = k(n-k)a^2b^{-1}n^{-2}$.

For a moment we shall impose no restriction on n and k.

LEMMA 2. Let S be such that

$$S^k \equiv -(n-k)b^{-1}an^{-1} \quad \text{and} \quad S^n \equiv -(n-k)b^{-1}k^{-1} .$$

If $R \equiv S^{-1}$ then $f(R) \equiv f'(R) \equiv 0 \bmod \mathcal{I}$ and $S_1 = S$.

PROOF. In fact

$$R^n - aR^k - b \equiv bk[-(n-k)]^{-1} - a[-(n-k)^{-1}ba^{-1}n] - b \equiv$$

$$\equiv -(n-k)^{-1} b[k-n+n-k] \equiv 0 \bmod \mathcal{I} .$$

and from $f'(X) = nX^{n-1} - akX^{k-1} = X^{k-1}(nX^{n-k} - ka)$ and

$$n(kan^{-1})-ka \equiv 0 \bmod \mathcal{I} \Longrightarrow f'(R) \equiv 0 \bmod \mathcal{I}. \quad \blacksquare$$

<u>LEMMA 3</u>. If $f(R) \equiv f'(R) \equiv 0 \bmod I \Longrightarrow R^k \equiv -bna^{-1}(n-k)^{-1}$ and $R^n \equiv -bk(n-k)^{-1}$.

<u>PROOF</u>. In fact, g.c.d. $(\mathcal{I},b) = 1$ and $f(R) \equiv 0$ implies $R \not\equiv 0 \bmod \mathcal{I}$, and R regular. From $f'(R) \equiv 0$ we get $R^{n-k} \equiv kan^{-1}$ and from $f(R) \equiv R^{-k}(R^{n-k} - a - R^{-k}b) \Longrightarrow R^{-k}b \equiv -kan^{-1}+a \equiv -(n-k)an^{-1}$ or $R^k \equiv -(n-k)an^{-1}b^{-1}$. $\blacksquare$

<u>REMARK 4</u>. Let us now look at the case where $n > 2k$. We shall assume that g.c.d. $(\mathcal{I},b) = 1$. We can write:

$$F(y) = -f(bX^{-1})X^{-n}b^{n-1} \equiv y^n + ab^{k-1}y^{n-k} - b^{n-1}$$

with $n > 2(n-k)$. If we call R' its root modulo $\mathcal{I}$, (given by Lemma's 1 and 2), then

$$F(y) \equiv (y-R')^2 p(y) \bmod \mathcal{I} \quad \text{and} \quad p(R') \not\equiv 0.$$

Now

$$f(X) \equiv -X^n b^{-(n-1)} F(\tfrac{b}{X}) = (X - b(R')^{-1})^2\, p_1(X). \text{ We set}$$

$R \equiv b(k')^{-1}$. As $p(R') \not\equiv 0 \Longrightarrow p(R) \equiv 0$ modulo $\mathcal{I}$, since

$p_1(X) = X^n(b^{-n-1})p(b/X)$. Hence $f(X) \equiv (X-R)^2\, p_1(X) \bmod \mathcal{I}$. Consequently Lemma 3 applies. $\blacksquare$

Now we set $\mu(j) = -(n-k)k^{-1}$, $0 \leq j < k$ and $\mu(j) = 1$ otherwise. Let

$$g(X) = [X^n - R^n - a(X^k - R^k)]/(X-C) = \sum_{i=0}^{n-1} R^{n-i-1}X^n - a\sum R^{k-v-1}X^i \equiv$$

$$\equiv \sum_{i=k}^{n-1} R^{n-i-1}X^i + \sum_{i=0}^{k-1}(R^{n-i-1} - aR^{k-i-1})X^i = \sum_{i=0}^{n-1} \mu^*(j)R^{n-i-1}X^i ,$$

where $\mu^*(j) = 1$ if $i \geq k$ and $\mu^*(j) = 1 - aR^{k-n} \equiv 1 - aS^{n-k} \equiv$ $\equiv 1 - ak^{-1}a^{-1}n \equiv -(n-k)k^{-1} \bmod \mathcal{I}$. Hence $\mu(j) = \mu^*(j)$ for a $0 \leq j \leq n-1$.

<u>LEMMA 5</u>. Let R satisfy the congruences $R^k \equiv -bna^{-1}(n-k)^{-1}$ and $R^n \equiv -(n-k)^{-1}bk$. If $n > 2k$, then $\{\lambda^*(j)\}$, $\lambda^*(j) =: \mu(j)R^{n-i-1}$ satisfies the trace congruences.

<u>PROOF</u>. We first observe that $R^{n-k} \equiv kan^{-1}$. Let us now verify our congruences.

VERIFICATION OF (I):

$$n\lambda^*(0) + (n-k)a\lambda^*(n-k) = n(-(n-k)k^{-1})R^{n-1} + (n-k)aR^{n-(n-k)+1} \equiv$$
$$\equiv (n-k)R^{n-1}[-nk^{-1} + aR^{-(n-k)}] \equiv 0 \bmod \mathcal{I}.$$

VERIFICATION OF (II):

We first observe that for $j=1,\dots,n-2k$, both $n-j$, $n-k-j \geq k$ (for $n-j \geq n-(n-2k) = 2k$ and $n-k-j \geq n-k-(n-2k) = k$). Now

$$nb\lambda^*(n-j) + (n-k)a\lambda^*(n-k-j) = nbR^{n-1-(n-j)} + (n-k)aR^{n-1-(n-k-j)} \equiv$$
$$\equiv R^{j-1}[nb + (n-k)aR^k] \equiv R^{j-1}[nb + (n-k)a(-1)bna^{-1}(n-k)^{-1}] \equiv 0$$
mod $\mathcal{I}$.

VERIFICATION (III):

We have, for $\ell = 1,\dots,k \geq 1$:

$$(n-k)a\lambda^*(k-\ell) + nb\lambda^*(2k-\ell) + (n-k)a^2\lambda^*(n-\ell) \equiv (n-k)aR^{n-1-(k-\ell)}\cdot$$
$$\cdot(-1)(n-k)k^{-1} + nbR^{n-1-(2k-\ell)} + (n-k)a^2R^{n-1(n-\ell)} \equiv$$
$$\equiv R^{n-1+\ell}[(-1)(n-k)^2ak^{-1}R^{-k} + nbR^{-2k} + (n-k)a^2R^{-n}] \equiv$$
$$\equiv R^{n-1+\ell}[(-1)(n-k)^2ak^{-1}(-1)b^{-1}n^{-1}a(n-k) + nbb^{-2}n^{-2}a^2(n-k)^2 +$$
$$+ (n-k)a^2(-1)(n-k)b^{-1}k^{-1} \equiv$$
$$\equiv R^{n-1+\ell}(n-k)^2a^2b^{-1}n^{-1}[(n-k)k^{-1} + 1 - (-1)nk^{-1}]$$
and $(n-k)k^{-1} + 1 + (-1)nk^{-1} \equiv k^{-1}[n-k+-n] \equiv 0 \bmod \mathcal{I}$.

Here we used the fact that $k-\ell < k$, $2k-\ell \geq k$ and $n-\ell \geq k$, for $1 \leq \ell \leq k$.

This concludes our verification in $k=1$.

VERIFICATION OF (IV):

We have

$$nb\lambda^*(k-\ell) + (n-k)a^2\lambda^*(n-k-\ell) + (2n-k)ab\lambda^*(n-\ell) \equiv$$

$$\equiv nb(-1)(n-k)k^{-1}R^{n-1-k-\ell} + (n-k)a^2R^{n-1-(n-k-\ell)} + (2n-k)abR^{n-1-(n-\ell)} \equiv$$

$$\equiv R^{n-1+\ell}[(-1)nb(n-k)k^{-1}R^{-k} + (n-k)a^2R^{-(n-k)} + (2n-k)abR^{-n}] \equiv$$

$$\equiv R^{n-1+\ell}[(-1)nb(n-k)k^{-1}b^{-1}n^{-1}a(n-k) + (n-k)a^2k^{-1}a^{-1}n +$$

$$+ (2n-k)ab(-1)b^{-1}k^{-1}(n-k)] \equiv$$

$$\equiv R^{n-1+\ell}(n-k)k^{-1}a[n-k+n-(2n-k)] \equiv 0 \mod \mathcal{I}.$$

This calculation is valid as long as $n-k-\ell$, $n-\ell \geq k$, and if $n \geq 3k-1$ this holds for all $1 \leq \ell \leq k-1$ because here $n-k-\ell \geq n-k-(n-2k) = k$, and $n-\ell \geq n-(n-2k) = 2k$. This concludes our verification of (IV) and of the case $n \geq 3k-1$.

Finally let us verify (V), when $2k \leq n < 3k-1$. We have

$$nb\lambda^*(\ell) + (2n-k)ab\lambda^*(n-k+\ell) + (n-k)a^2\lambda^*(n-2k+\ell) +$$

$$+ (n-k)a^3\lambda^*(2n-3k+\ell) \equiv nbR^{n-1-\ell}(-1)(n-k)k^{-1}$$

$$+ (2n-k)abR^{n-1-(n-k+\ell)} + (n-k)a^2(-1)(n-k)k^{-1}R^{n-1-(n-2k+\ell)} +$$

$$+ (n-k)a^3R^{n-(2n-3k+\ell)-1} \equiv R^{-\ell-1}(n-k)[(-1)k^{-1}nbR^n +$$

$$+ (2n-k)ab(n-k)^{-1}R^k + (n-k)a^2(-1)k^{-1}R^{2k} + a^3R^{3k-n} \equiv$$

$$\equiv R^{-\ell-1}(n-k)[(-1)k^{-1}nb(-1)(n-k)^{-1}kb + (2n-k)ab(n-k)^{-1}(-1)bna^{-1}(n-k)^{-1} -$$

$$+ (n-k)(-1)a^2k^{-1}b^2n^2a^{-2}(n-k)^{-2} + a^3(-1)b^3n^3a^{-3}(n-k)^{-3}(-1)(n-k)b^{-1}k^{-1}] \equiv$$

$$\equiv R^{-\ell-1}(n-k)^{-1}b^2nk^{-1}[(n-k)k-(2n-k)k-n(n-k)+n^2] \equiv 0 \mod \mathcal{I}.$$

This concludes our verification. ∎

We shall close this paragraph with a

<u>LEMMA 6</u>. Let g.c.d. $(n,k) = 1$. If we can find and ideal $\mathcal{I}$, g.c.d. $(\mathcal{I}, nk(n-k)ab) = 1$, and $S \in \mathcal{R}$ such that

$$S^k \equiv -(n-k)ab^{-1}n^{-1} \quad \text{and} \quad S^n \equiv -(n-k)b^{-1}k^{-1} \mod \mathcal{I}$$

then $R = S^{-1}$ is a double root of f mod $\mathcal{I}$ and $\mathcal{I}$ divides $\Delta(x)$.

<u>PROOF</u>. In fact, we can find u' and v' such that $u'k + v'u = 1$ and necessarily $(S^k)^{u'}(S^n)^{v'} \equiv S \mod \mathcal{I}$ (i.e. take $u' = u+sv$, $v' = -v$). By repeating the argument of Lemma 1 we get $C \equiv S^k \equiv \rho C$, hence $\rho \equiv 1$ and this is equivalent to $\mathcal{I} | \Delta(x)$. ∎

3.7. SECOND MAIN THEOREM

Now we put together our results:

<u>THEOREM</u>. Let $f(X) = X^n - aX^k - b$, $a,b \in \mathcal{R}$, and let $\mathcal{I}$ be an ideal of $\mathcal{R}$ such that $\mathcal{I}|\Delta(x)$, and g.c.d. $(\mathcal{I}, n(n-k)ab) = 1$. Then

(1) $D(S'_{\mathcal{I}}/K)$ is square free and $S'_{\mathcal{I}} = \mathcal{R}_{\mathcal{I}}[x]$ iff (x) is square free as ideal of $\mathcal{R}_{\mathcal{J}}$.

(2) If $\mathcal{I} = \mathcal{J}^2\mathcal{I}^*$, $\mathcal{I}^*$ square in $S'_{\mathcal{J}}$, then $S'_{\mathcal{I}} = \mathcal{R}_{\mathcal{I}} + \ldots + \mathcal{R}_{\mathcal{I}}x^{n-2} + \mathcal{I}^{-1}z$, $z = g(x)$, and $D(S'_{\mathcal{I}}/K) = \mathcal{I}^*$.

<u>PROOF</u>. Let $n > 2k$. We have proved that up to a multiplicative constant the trace congruences have a unique solution modulo $\mathcal{I}$. As the coefficients of $g(x)$ satisfy these congruences we have that $g(x) = \lambda x$ for some $\lambda \in \mathcal{R}_{\mathcal{I}}$. By Theorem 1, $\alpha z \in S'_{\mathcal{I}}$ for all $\alpha \in \mathcal{J}^{-1}$ if $\mathcal{I} = \mathcal{J}^2\mathcal{I}^*$, consequently $D(S'_{\mathcal{I}}/K) = \mathcal{I}^*$.

Finally if $n < 2k$, then b being an unit in $\mathcal{R}_{\mathcal{I}}$, x is also an unit and we can apply our results to $F(y)=y^n k+ab^{k-1}y^{n-k}-b^{n-1}$ and here we also have g.c.d. $(\mathcal{I}, nkab) = 1$. Also $(\Delta(x)) = (\Delta(y))$ in $\mathcal{R}_{\mathcal{I}}$. Now Δ is square free iff $S'_{\mathcal{I}} = \mathcal{R}_{\mathcal{I}}[y]$ and $S'_{\mathcal{I}} = \mathcal{R}_{\mathcal{I}}[x]$, because if Δ is not square free $S'_{\mathcal{I}} = \mathcal{R}_{\mathcal{I}}(x, \mathcal{J}^{-1}z)$, and $D(S'_{\mathcal{I}}/K) = \mathcal{I}^*$. We set $g^*(x) = x^{n-1}z(y) \in S'_{\mathcal{I}}$ and if one compute the DS'_o for $S'_o = \mathcal{R}_{\mathcal{I}} + \ldots + \mathcal{R}_{\mathcal{I}}x^{n-2} + \mathcal{J}^{-1}g^*(x)$ one sees that $DS'_o = (\Delta(x))/\mathcal{J}^2 = \mathcal{J}^*$. Therefore $S'_{\mathcal{I}} = S'_o$. ∎

As a final remark we have:

<u>REMARK</u>. We can state our theorem with $\mathcal{I} = (\Delta(x))$ and find lattice bases for S' over $\mathcal{R}$. Other interesting situation is $f(X) = X^n - naX^k + (n-k)b$ where $\Delta(x) = \pm b^{k-1}(n-k)^{n-k}n^n[k^k a^n - b^{n-k}]$ and here for all $\mathfrak{p}|k^k a^n - b^{n-k}$, we have $0 \le v_{\mathfrak{p}}(D(S'/K)) \le 1$.

REFERENCES

Allan , N. (1982) - On the ring of integers of $y^n = ay + b$. Proceeding of VI ELAM , Morelos , Mexico, p. 123/130.

Komatsu, K. - Integral bases in Algebraic Number Fields. Journal für Mathematik, band 278/279, Berlin, 1975, p. 137/144.

Uchida, K. - Unramified Extensions of Quadratic Number Fields, II. Tôhoku Mathematical Journal, volume 22, Tôhoku, 1970, p. 220/224.

Allan, N. (1988) - On Integral bases of some ring of integers - Anais da Academia Brasileira de Ciências, (to appear).

RELATÓRIOS TÉCNICOS — 1988

01/88 – **A Linear Continuous Transportation Problem** – *Enrique D. Andjel, Tarcisio L. Lopes* and *José Mario Martinez.*

02/88 – **A Splitting Theorem for Complete Manifolds With Non-Negative Curvature Operator** – *Maria Helena Noronha.*

03/88 – **Mathematical Physics of the Generalized Monopole without String** – *W. A. Rodrigues Jr., M. A. Faria-Rosa, A. Maia Jr.* and *E. Recami.*

04/88 – **A Family of Quasi-Newton Methods with Direct Secant Updates of Matrix Factorizations** – *José Mário Martinez.*

05/88 – **Rotation Numbers of Differential Equations. A Framework in the Linear Case** – *Luiz San Martin.*

06/88 – **A Geometrical Theory of non Topological Magnetic Monopoles** – *Marcio A. Faria-Rosa* and *Waldyr A. Rodrigues Jr.*

07/88 – **Cosmic Walls and Axially Symmetric Sigma Models** – *Patricio S. Letelier* and *Enric Verdaguer.*

08/88 – **Verificação do Nível de Enlace do Protocolo X-25** – *Célio C. Guimarães* e *Edmundo R. M. Madeira.*

09/88 – **A Numerically Stable Reduced-Gradient Type Algorithm for Solving Large-Scale Linearly Constrained Minimization Problems** – *Hermínio Simões Gomes* and *José Mário Martínez.*