On Subalgebras of Free Lie Algebras and on the Lie Algebra Associated to the Lower Central Series of a Group

by

Tomasz Stefanicki

Department of Mathematics and Statistics
McGill University, Montreal

November 1987

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics

ISBN 0-315-45943-3

On Subalgebras of Free Lie Algebras and on the Lie Algebra Associated to the Lower Central Series of a Group

Abstract

The main purpose of the first part of this thesis is to answer the question: "When is a subalgebra of a free Lie algebra free"? In the second part we determine the Lie algebra associated to the lower central series of a group in the case where the defining relators satisfy certain independence conditions. In the third part, we give some criteria for elements of the Lie algebra to be strongly free.

Sur certaines sous–algèbres d'algèbres de Lie libres, et sur l'Algèbre de Lie associée à la série inférieure centrale d'un groupe

Résumé

Le but principal de la première partie de cette thèse est de déterminer les conditions suffisantes pour rendre libre une sous–algèbre d'une algèbre de Lie libre.

Dans la deuxième partie on determine l'algèbre de Lie associée à la série inférieure centrale d'un groupe, dans le cas où les relations definissantes satisfont certaines conditions d'indépendance.

Dans la troisième partie on donne quelques critères pour que les élements de l'algèbre de Lie soient fortement libres.

Acknowledgements

I am indebted primarily to Professor John P. Labute, without whose inspiration, advice and support this work would have been impossible. Thanks are also due to Professor R. Moody and Professor A. Pianzola who were my teachers in the Lie algebra course given in 1985–86 in Montreal.

I also thank Professor P. Russell for the financial help he gave me through his research funds.

I thank Mrs. S. Wright and Mr. C. Hennings for consultation on German.

I thank Ms. P. Eiteman for typing the manuscript with so much care.

Finally, my thanks go to my parents with gratitude.

TABLE OF CONTENTS

Introduction

In the second chapter of this thesis we are trying to answer the following question: "When is a subalgebra of a free Lie algebra free?". Witt [15] and Siršov [14] showed that every subalgebra H of a free Lie algebra L over a field k is free. The main idea of Witt's proof comes from Schreier's proof that every subgroup of a free group is free. Sirsov used in his proof a k–basis of L constructed by M. Hall [6]. When k is not a field but any commutative ring with unity, the above mentioned theorem is no longer valid as even very simple examples can show. Witt in [15] showed that if k is the ring of integers and H is a homogeneous subalgebra with respect to some N–grading of L, then if the abelian group L/H is free, H is a free Lie algebra. This result can be slightly extended. To be able to apply the idea of his proof, all we need to know is that certain k–submodules of L are free. To ensure it, we can assume that k is a commutative ring with a property that every projective k–module is free. However, we still need to assume that H is a homogeneous subalgebra with respect to some N–grading of L since the argument given by Sirsov does not work if k is not a field. We use the result of [15] in the third chapter of this thesis where we study the algebras associated to the lower central series of groups. Labute showed [10], that the Lie algebra associated to the descending central series of a finitely presented group is a finitely presented Lie algebra if the relators satisfy certain independence conditions (the proof uses the results of [7] and [8]):

Let F be a free group on $\{X_1,\ldots,X_N\}$ and let $r_1,\ldots,r_M$ be any elements of F.

Let R be the normal subgroup generated by $\{r_1,\dots,r_M\}$. Let L be the free Lie algebra associated to the lower central series of F, and let g be the Lie algebra associated to the lower central series of $G = F/R$. Let τ be the ideal of L generated by the initial forms $\rho_1,\dots\rho_M$ of $r_1,\dots,r_M$ in L. He proves that if:

1) L/τ is a free abelian group and

2) $\tau/[\tau,\tau]$ is a free $U(L/\tau)$–module

then $g = L/\tau$, where $U(L/\tau)$ denotes the universal enveloping algebra of L/τ.

If conditions (1) and (2) are satisfied, following terminology introduced by Anick ([1] and [2]), we call the elements $\rho_1,\dots\rho_M$ strongly free (or inert).

In the second part of Chapter III we show some criteria for the elements $\rho_1,\dots,\rho_M$ to be strongly free. We show that if $\rho_1,\dots,\rho_M$ are homogeneous elements of a free Lie algebra $L(\xi_1,\dots,\xi_N)$ over a P.I.D. then:

If $\chi_{U(L/\tau)(P)} = \chi_{U(L)}/1 + (t^{d_1}+\dots+t^{d_M})\chi_{U(L)}$ for every maximal ideal (P) of k, then $\rho_1,\dots,\rho_M$ are strongly free, where d_i = degree of ρ_i in L, χ_A–Euler–Poincaré series of a locally finite connected graded algebra A ([2]) and $U(L/\tau)(P) = U(L/\tau)\otimes_k k/(P)$.

This reduces the problem to the case when k is a field. Anick showed [2] that if $\alpha_1,\dots\alpha_M$ are homogeneous elements of a free associative algebra $Ass(\xi_1,\dots,\xi_N)$ then:

$\hat{\alpha}_1,\dots,\hat{\alpha}_M$ combinatorially free ([2]) implies that $\alpha_1,\dots,\alpha_M$ are strongly free where $\hat{\alpha}_i$ denotes the highest term of α_i with respect to some lexicographic order of the free monoid $M(\xi_1,\dots,\xi_N)$. Using these two results, we treat some interesting examples.

Chapter I

Preliminaries

In this chapter we will introduce the concepts which will be necessary to prove the results in Chapter II and III. Most of the material contained in this chapter is classical and can be found in numerous places in the Literature. We will always give the main references for each section, writing them in square brackets [...]. The key statements for the theory will be proved in more detail to make this work self contained, whereas the statements which are either basic or of less importance for the theory will be given outlines rather than detailed proofs. This chapter is divided into several sections to make later reference easier. In Section 1 we define basic concepts. In Section 2, we prove a very important theorem of Birkhoff–Witt and we show some basic consequences of it. In Section 3, we define and construct a free Lie algebra and we prove some important theorems about free Lie algebras which we will refer to later. In Section 4, we associate a Lie algebra to a lower central series of a group. In this chapter, the letter k denotes a commutative ring with unity. In §4, k will be assumed to be the ring of integers and we will denote it by the letter Z. Unless otherwise mentioned, all algebras, all modules and all tensor products are over k.

§1. Basic definitions

The main references for this section are [3], [4], [5] [10] and [13]. By a k–algebra or algebra over k we mean a k–module together with a k–bilinear map

$$A \times A \longrightarrow A$$

(i.e., a k–homomorphism $A \otimes_k A \longrightarrow A$).

Definition I.1.1.

A Lie algebra over k is an algebra with the following properties: if $[x,y]$ denotes the image of (x,y) under the map $A \times A \longrightarrow A$ then,

(L1) $[x,x] = 0$ for all $x \in A$.

(L2) $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$ for all $x,y,z \in A$.

The identity of (L2) is called the Jacobi identity and we shall denote its left hand side by $Jac(x,y,z)$. It is a long established custom to call the expression $[x,y]$ the bracket or commutator of x and y. It is useful to note that to establish that an algebra A is a Lie algebra, it suffices to verify that the conditions (L1) and (L2) hold for all x,y,z in some generating set of the k–module A. It is customary to denote Lie algebras using the letters L, H, g, n or τ and we will adhere to this convention except where common usage has established otherwise.

Example I.1.1.

(i) Let g be any k–module. Define $[x,y] = 0$ for all $x,y \in g$. Such a g is called an abelian Lie algebra.

(ii) Let A be an associative algebra over k and define $[x,y] = x \cdot y - y \cdot x$ for all $x,y \in A$ (where $x \cdot y$ is the product of x and y in A). Then A, taken as a k–module together with this new composition law becomes a Lie algebra. We will denote this algebra by Lie (A) and call it the Lie algebra of the associative algebra A.

A subset h of a Lie algebra g is called a Lie subalgebra of g if it is a k–module and is closed under the bracket multiplication, i.e., if $[x,y] \in h$ whenever $x,y \in h$.

A subset a of a Lie algebra g is called an ideal of g if it is a k–module and if for all $x \in \mathfrak{a}$ and for all $y \in \mathfrak{g}$, $[y,x] \in \mathfrak{a}$. The formula (L1) tells us that then $[x,y] \in \mathfrak{a}$ for all $x \in \mathfrak{a}$ and $y \in \mathfrak{g}$.

A mapping $f: \mathfrak{g} \to \mathfrak{h}$ from one Lie algebra into another is called a homomorphism if it is k–linear and $f([x,y]) = [f(x),f(y)]$ for all $x,y \in \mathfrak{g}$.

Let A be an algebra and let X and Y be subsets of A. We define $X \cdot Y$ (or $[X,Y]$ if A is a Lie algebra) to be the set of all finite sums of products $x \cdot y([x,y])$ where $x \in X$ and $y \in Y$. If X or Y is empty then $X \cdot Y([X,Y]) = \emptyset$ by definition. Notice that $A \cdot A([A,A])$ is always an ideal of A. When A is a Lie algebra $[A,A]$ is called the derived algebra of A.

Let V be a k–module. The tensor algebra of V denoted by T(V) is a k–module

$$T(V) = \bigoplus_{n \geq 0} T^n(V) \text{ where } T^n(V) = V \otimes \ldots \otimes V = \overset{n}{\otimes} V$$

with a multiplication definied through the natural isomorphisms

$$(\overset{p}{\otimes} V) \otimes (\overset{q}{\otimes} V) \cong \overset{p+q}{\otimes} V.$$

For any associative algebra A with a unit, one has:

$$\mathrm{Hom}_{Mod}(V,A) = \mathrm{Hom}_{Ass}(T(V),A).$$

Let V be a k–module. The symmetric algebra of the k–module V, denoted by S(V) is defined to be the biggest commutative quotient of T(V) i.e., $S(V) = T(V)/J$, where J is an ideal of T(V) generated by all elements of the form $v \otimes w - w \otimes v$ for all $v,w \in V$.

Let V be a k–module and M an additive monoid. By a grading of V by M we will understand a family $(V_\alpha)_{\alpha \in M}$ of submodules of V such that

$$V = \bigoplus_{\alpha \in M} V_\alpha.$$

Given such a grading we will say that V is graded by M or M–graded. For each $\alpha \in M$ we call V_α a homogeneous submodule of degree α. If $v = \Sigma v_\alpha \in V$, $v_\alpha \in V_\alpha$, then v_α is called the homogeneous component of degree α. An element lying in a homogeneous submodule V_α is said to be homogeneous of degree α. Notice that in this sense, 0 is homogeneous of every degree.

Let A be an algebra over k and let $(A_\alpha)_{\alpha\in M}$ be a M–grading of A (as a k–module). We say that the grading is compatible with the algebra structure of A and that A is M–graded algebra if

$$A_\alpha \cdot A_\beta \subset A_{\alpha+\beta} \text{ for all } \alpha,\beta \in M.$$

Let W be a k–submodule of an M–graded k–module V. For each $\alpha \in M$ define $W_\alpha = V_\alpha \cap W$. We say that W is a graded submodule of V if $W = \bigoplus_{\alpha\in M} W_\alpha$. It is useful to note that to say that W is a graded submodule of V is equivalent to saying that whenever $w = \Sigma v_\alpha \in W$ then each homogeneous component $v_\alpha \in W$. If W is a graded submodule of V then the quotient module V/W has an inherited grading with $(V/W)_\alpha = V_\alpha/W_\alpha$.

Let $A = \bigoplus_{\alpha\in M} (A)_\alpha$ be a graded algebra. An ideal J of A is called a graded ideal if J is a graded submodule of A. If J is a graded ideal of A then the quotient module $A/J = \bigoplus_{\alpha\in M} (A/J)_\alpha$ is graded compatibly with its algebra structure, that is

$$(A/J)_\alpha \cdot (A/J)_\beta \subset (A/J)_{\alpha+\beta}$$

for all $\alpha,\beta \in M$. If $S \subset A$ is any subset of homogeneous elements of A then both the subalgebra and the ideal of A generated by S are also homogeneous.

<u>Definition I.1.2.</u>

Let g be a Lie algebra and V a k–module. By a <u>representation</u> of g on V we will mean a Lie algebra homomorphism $\Pi:g \longrightarrow \mathrm{Lie}(\mathrm{End}_k(V))$. In other words, Π is a k–linear map from g into $\mathrm{End}_k(V)$ (the algebra of endomorphisms of a k–module V) satisfying

$$\Pi([x,y])\cdot(v) = \Pi(x)\cdot\Pi(y)\cdot(v) - \Pi(y)\cdot\Pi(x)\cdot(v) \quad \text{for all } x,y \in g \text{ and } v \in V.$$

Definition I.1.3.

By an action of a Lie algebra g on a k–module V we will understand a bilinear mapping

$$g \times V \longrightarrow V \; ((x,v) \longrightarrow x\cdot v \quad \text{for all } x \in g,\, v \in V) \text{ satisfying}$$
$$[x,y]\cdot v = x\cdot y\cdot v - y\cdot x\cdot v \quad \text{for all } x,y \in g \text{ and } v \in V.$$

Given an action, we say that g acts on V and V is then called a g–module (relative to this action).

These two concepts (modules and representations) are essentially the same. If g acts on V, then $v \longrightarrow x\cdot v$ is a k–linear mapping of V into itself and we can define a representation $\Pi:g \longrightarrow \mathrm{End}_k(V)$ by $\Pi(x)\cdot(v) = x\cdot v$. On the other hand, if Π is a representation of g on V then g acts on V via

$$x\cdot v = \Pi(x)\cdot(v) \quad \text{for all } x \in g \text{ and } v \in V.$$

Definition I.1.4.

Let A be an algebra over k. A derivation $D:A \longrightarrow A$ is a k–linear map with the property: $D(x\cdot y) = D(x)\cdot y + x\cdot D(y)$ for all $x,y \in A$.

Example I.1.2.

The set Der(A) of all derivations of an algebra A is a Lie algebra with the product $[D,D'] = D\cdot D'+D'\cdot D$ (easy computation). Let g be a Lie algebra. For any $x \in g$ define a map $\mathrm{ad}x:g \longrightarrow g$ by $\mathrm{ad}x(y) = [x,y]$. Then as a consequence of the Jacobi identity the map adx is a derivation of g and the map ad defined by $ad(x) = adx$ is a Lie homomorphism of g into $Der(g)$. We see that ad is a representation of g on $End_k(g)$. It is called the adjoint representation of g. The corresponding g–module is g itself where the action is given by left multiplication.

Let $g = \bigoplus_{\alpha\in M} g_\alpha$ be an M–graded Lie algebra. If V is a g–module we say that an M–grading $(V_\alpha)_{\alpha\in M}$ of the module V is compatible with the module structure if

$$g_\beta V_\alpha \subset V_{\beta+\alpha} \text{ for all } \beta,\alpha\in M.$$

If this is the case we then say that V is a graded g–module.

Let V be a g–module and $W \subset V$ a g–submodule of V. The quotient k–module V/W can be given a natural g–module structure by defining

$$x\cdot\overline{v} = \overline{x\cdot v} \text{ for all } x\in g,\ v\in V$$

where $\overline{}: \longrightarrow V/W$ is the canonical map. This module is called the quotient module of V by W.

Definition I.1.5.

Let g be a Lie algebra over k. By universal envelope algebra of g we will understand a pair $(U(g),i)$ composed of an associative algebra with unity $U(g)$ together with a map $i:g \longrightarrow U(g)$ satisfying the following conditions:

(U1) The map i is a Lie algebra homomorphism from g into Lie $(U(g))$, that is i is a k–linear and $i([x,y]) = i(x)i(y) - i(y)\cdot i(x)$ for all $x,y \in g$.

(U1) If A is any associative algebra with unity and f is any Lie algebra homomorphism $f:g \longrightarrow Lie(A)$, there exists unique algebra homomorphism $\overline{f}:U(g) \longrightarrow A$ which extends f, that is $f = \overline{f}\cdot i$. In other words, there is an isomorphism

$$Hom_{Lie}(g,Lie(A)) \cong Hom_{Ass}(U(g),A).$$

It is trivial that $U(g)$, if it exists, is unique up to unique isomorphism. To show its existence we use the tensor algebra $T(g)$ of g. Let I be the two-sided ideal of $T(g)$ generated by the elements of the form $[x,y]-x\otimes y + y\otimes x$, for all $x,y \in g$. We claim that the quotient algebra $U(g) = T(g)/I$ together with the map $i:g \to U(g)$ which is the composition $g \to T^1(g) \to T(g) \to U(g)$, satisfy conditions (U1) and (U2). Indeed, let f be any Lie algebra homomorphism from g into a Lie algebra Lie (A) of an associative algebra A. It extends to unique homomorphism $\Psi:T(g) \to A$. Since $\Psi(I) = 0$, Ψ defines $\bar{f}:U(g) \to A$.

Remark. Let g be a Lie algebra and Π a representation of g into a k-module V. Thus Π is a Lie algebra homomorphism from g into $Lie(End_k(V))$. It follows that Π extends to an algebra homomorphism $\bar{\Pi}$ form $U(g)$ into $End_k(V)$. In other words, V becomes a left $U(g)$-module with the action $u\cdot v = \bar{\Pi}(u)\cdot(v)$ for all $u \in U(g)$ and $v \in V$. Conversely if V is a left $U(g)$-module, we retrieve a representation Π of g on V by defining $\Pi(x)\cdot(v) = i(x)\cdot v$ (where $i:g \to U(g)$ is the canonical map). It is easy to verify that these two procedures are inverses of each other and hence one obtains an isomorphism of the category of g-modules onto the category of left $U(g)$-modules.

Some of the functorial properties of universal enveloping algebras are the following:

(I.1.1) If $g = g_1 \times g_2$, where g_1 and g_2 are Lie algebras which commute then

$$U(g) = U(g_1)\otimes_k U(g_2) \text{ as k-modules.}$$

(I.1.2) Let K_1 be an extension ring of k and let $g_{(K_1)} = g\otimes_k K_1$, then

$$U(g_{(K_1)}) = U(g)\otimes_k K_1 \overset{def}{=} U(g)_{(K_1)}.$$

(I.1.3) Let $\mathfrak{a}$ be an ideal of g, f the canonical homomorphism of g onto $g/\mathfrak{a}$. Then the homomorphism $\bar{f}:U(g) \longrightarrow U(g/\mathfrak{a})$ defined canonically by f is surjective and its Kernel is the ideal $I(\mathfrak{a})$ of $U(g)$ generated by $i(\mathfrak{a})$ where $i:g \longrightarrow U(g)$ is the canonical map.

Proof of (I.1.1).

The map $f:(x_1,x_2) \longrightarrow i_1(x_1)\otimes 1 + 1\otimes i_2(x_2)$ (i_k is the canonical map $i_k:g_k \longrightarrow U(g_k)$ $k = 1,2$, $x_1 \in g_1$, $x_2 \in g_2$) from g into $U(g_1)\otimes U(g_2)$ is a Lie algebra homomorphism since g_1 and g_2 commute. Hence f induces an associative algebra homomorphism $\bar{f}:U(g) \longrightarrow U(g_1)\otimes_k U(g_2)$. The homomorphisms $g_k \longrightarrow g \longrightarrow U(g)$ $k = 1,2$, induce homomorphism $\varphi_k:U(g_k) \longrightarrow U(g)$ $k = 1,2$, and since g_1 and g_2 commute we have that $\varphi_1(x_1)\cdot\varphi_2(x_2) = \varphi_2(x_2)\cdot\varphi_1(x_1)$ for all $x_1 \in g_1$ and $x_2 \in g_2$. Let $\bar{\varphi}:U(g_1)\otimes U(g_2) \longrightarrow U(g)$ be given by $\bar{\varphi}_1(x_1\otimes x_2) = \varphi_1(x_1)\varphi_2(x_2)$, then we have $\bar{f}\cdot\bar{\varphi} = \text{id}$ and $\bar{\varphi}\cdot\bar{f} = \text{id}$.

q.e.d.

Proof of (I.1.2).

If V is a k–module we define $V_{(K_1)} = V\otimes_k K_1$. The tensor algebra of $g_{(K_1)}$ is canonically identified with $T(g)_{(K_1)}$. Let I be the ideal of $T(g)$ generated by the elements of the form $[x,y] - x\otimes y + y\otimes x$ for all $x,y \in g$, and let I_1 be the ideal of $T(g)_{(K_1)}$ generated by the elements of the form $[x',y'] - x'\otimes y' + y'\otimes x'$ for all $x',y' \in g_{(K_1)}$. Clearly the canonical image of $I_{(K_1)}$ in $T(g)_{(K_1)}$ is contained in I_1. Now, let $x' = \sum_i x_i\otimes k_i$, $y' = \sum_j y_j\otimes L_j$ be in $g_{(K_1)}$ (x_i,y_j in g; k_i, L_j in K_1). Then,

$$x'\otimes y' - y'\otimes x' - [x',y'] = \sum_{i,j}(x_i\otimes y_j - y_j\otimes x_i - [x_i,y_j])\otimes k_i\cdot L_j \quad .$$

which shows that I_1 is in fact equal the image of $I_{(K_1)}$ in $T(g)_{(K_1)}$. Hence, we see that $U(g)_{(K_1)} = (T(g)/I)_{(K_1)}$ can be canonically identified with $T(g)_{(K_1)}/I_1$ i.e., $U(g_{(K_1)})$ can be canonically identified with $U(g)_{(K_1)}$, and the canonical mapping $i_1: g_{(K_1)} \to U(g_{(K_1)})$ can be identified with $i\otimes id$, where i is the canonical map $g \to U(g)$.

q.e.d.

Proof of (I.1.3).

Let $\varphi: \mathfrak{a} \to g$ be the inclusion. It defines the homomorphism $\overline{\varphi}: U(\mathfrak{a}) \to U(g)$ such that $\overline{\varphi}\cdot i_1 = i\cdot\varphi$ where $i: g \to U(g)$ and $i_1: \mathfrak{a} \to U(\mathfrak{a})$ are canonical mappings. Since we have also $\bar{f}\cdot i = i_2\cdot f$ (where $i_2: g/\mathfrak{a} \to U(g/\mathfrak{a})$ is the canonical map), we see that $\bar{f}$ is zero on $I(\mathfrak{a})$. If Φ is the canonical homomorphism of $U(g)$ onto $U(g)/I(\mathfrak{a})$ we get the induced homomorphism $f_1: U(g)/I(\mathfrak{a}) \to U(g/\mathfrak{a})$ such that $f_1\cdot\Phi = \bar{f}$. The mapping $\Phi\cdot i$ is a Lie algebra homomorphism and is zero on $\mathfrak{a}$. Hence, it defines a Lie algebra homomorphism θ of $g/\mathfrak{a}$ into $U(g)/I(\mathfrak{a})$ such that $\theta\cdot f = \Phi\cdot i$. The mapping θ induces the unique homomorphism f_2 of $U(g/\mathfrak{a})$ into $U(g)/I(\mathfrak{a})$ such that $\theta = f_2\cdot i_2$. Thus, $f_1\cdot\theta\cdot f = f_1\cdot\Phi\cdot i = i_2\cdot f$ and hence $f_1\cdot\theta = i_2$. Since $f_2\cdot f_1\cdot\theta = f_2\cdot i_2 = \theta$ and $f_1\cdot f_2\cdot i_2 = f_1\cdot\theta = i_2$ we see that $f_2\cdot f_1$ and $f_1\cdot f_2$ are the identity mappings of $U(g)/I(\mathfrak{a})$ and $U(g/\mathfrak{a})$ respectively.

q.e.d.

The universal enveloping algebra $U(g)$ is a supplemented k-algebra and therefore, following ([5], Chapter XIII) we define the homology groups of g as those of the supplemental algebra U(g) i.e.:

$$H_n(g,V) = \mathrm{Tor}_n^{U(g)}(V,k)$$

for any right g–module V. Let I(g) be the augmentation ideal of U(g) i.e., the kernel of the augmentation epimorphism $\epsilon: U(g) \to k$ induced by the map f from g into k defined by $f(x) = 0$ for all $x \in g$. The homology group $H_0(g,V)$ is the k–module $V \otimes_{U(g)} k$. Since $k \cong U(g)/I(g)$ we see that

$$H_0(g,V) = V/V \cdot I(g) = V/V \cdot g.$$

If g operates trivially on V (i.e, $V \cdot x = 0$ for all $v \in V$, $x \in g$) then

$$H_1(g,V) = V \otimes_k I(g)/I(g)^2.$$

The canonical map $i: g \to U(g)$ sends g into I(g) and [g,g] into $I(g)^2$ where [g,g] is the derived algebra of g. Hence, it induces a homomorphism $\bar{i}: g/[g,g] \to I(g)/I(g)^2$. On the other hand, we have the map $\varphi: T(g) \to g$ which is defined by $\varphi(T^1(g))$ = identity map, and $\varphi(T^n(g)) = 0$ for $n \neq 1$. The kernel of the composition map $\Pi \cdot \varphi$ where $\Pi: g \to g/[g,g]$, contains the ideal I of T(g) generated by the elements of the form $[x,y] - x \otimes y + y \otimes x$ for all $x,y \in g$. Hence, we obtain the induced homomorphism of U(g) into g/[g,g] which defines a map $\bar{\varphi}: I(g) \to g/[g,g]$. Clearly, the mappings $\bar{\varphi}$ and $\bar{i}$ are inverses of each other and hence we obtain an isomorphism

$$I(g)/I(g)^2 \cong g/[g,g].$$

Hence, if g operates trivially on V we can interpret the group $H_1(g,V)$ as $V \otimes_k g/[g,g]$.

Let h be an ideal of a Lie algebra g. If both h and g/h are free k–modules we will prove in the next section that U(g) regarded as a right U(h) module is free. As a consequence of it we get the Hochschild–Serre spectral sequence ([5], Chapter XV, p. 350):

$$H_n(g/h, H_m(h,V)) \underset{n}{\rightarrow} H_K(g,V).$$

We will use this sequence in Chapter II to give an alternative proof that certain subalgebras of free Lie algebras are free.

---

§2. Birkhoff–Will theorem

The main references for this section are [3], [4] and [13].

The key point in the proof of this theorem is the following proposition:

Proposition I.2.1.

Let g be a Lie algebra which is free as a k–module with a basis $\{x_i\}_{i\in I}$ where I is some well–ordered index set. Let T be any set. Then there exists a g–module F which is generated over g by the set T and whose k–basis consists of the elements of the form:

(*) $x_{i_1} \cdot \ldots \cdot x_{i_n} \cdot t$ with $i_1 \geq \ldots \geq i_n$, $n \geq 0$, $t \in T$.

Proof.

Let F be a free k–module with a k–basis the elements of the form (*). We denote the sequence $(x_{i_1},\ldots,x_{i_n})$ with $i_1 \geq \ldots \geq i_n$ by P and we will write $P \cdot t$ for the element $x_{i_1} \cdot \ldots \cdot x_{i_n} \cdot t \in F$ for all $t \in T$. We will also write $x_i \geq P$ if $i \geq i_1$ and $P' = x_i \cdot P$ will denote the sequence $(x_i, x_{i_1},\ldots,x_{i_n})$. The length of the sequence P will be denoted by $l(P)$. We want to make F a g–module. We will define the action of g on F by induction on $l(P)$ and for given $N = l(P)$ by reverse transfinite induction on the set I. If $l(P) = 0$ then define

$x\cdot Pt = x\cdot t$. If $x \geq P$ then define $x\cdot Pt = (xP)t$. Suppose that we have already defined g–action on F for all elements $Pt \in F$ with $l(P) < N$. Suppose also that we have already defined the action of the elements x_j with $j > i$ on all elements $Pt \in F$ with $l(P) = N$. We want to define the action of the element x_i on $P\cdot t \in F$ with $l(P) = N$ and in addition we want $x\cdot P\cdot t$ to be expressible as a fintie sum $\Sigma P_\alpha t$ with $l(P_\alpha) \leq l(P) + 1$. If $x_i \geq P$ then define

$$x_i\cdot P\cdot t = (x_i\cdot P)t \quad (t\in T).$$

If not, then define

$$(^{**}) \qquad x_i\cdot P\cdot t \doteq x_{i_1}\cdot(x_i\cdot P'\cdot t) + [x_i,x_{i_1}]\cdot P'\cdot t$$

where $P = (x_{i_1},\ldots,x_{i_N})$, $P' = (x_{i_2},\ldots,x_{i_N})$ and $i_1 \geq \ldots \geq i_N$. This action is well–defined by the induction hypothesis. Notice that $x_i\cdot P'\cdot t = P_1\cdot t + \sum_\alpha P_\alpha\cdot t$ where P_1 is the ordered sequence of elements $x_i, x_{i_1},\ldots,x_{i_N}$ and $l(P_\alpha) \leq l(P)$. In order to verify that this action defines a g–module structure on F we have to prove the following identity:

$$(^{***}) \qquad [x,y]\cdot P\cdot t = x\cdot(y\cdot P\cdot t) - y\cdot(x\cdot P\cdot t)$$

for all $x,y \in g$, and $t \in T$. We will do it by induction on the length $l(P)$ of P. Note that two sides of (***) are skew–symmetric. Hence, we can assume that $x > y$. If $x \geq P$, then the second term on the right hand side of (***) satisfies the conditions of (**) and hence (***) follows since by (**) we have

$$y\cdot(x\cdot P\cdot t) = x\cdot(y\cdot P\cdot t) + [y,x]\cdot P\cdot t.$$

Suppose that $x_{i_1} > x > y$ where $P = (x_{i_1},\ldots,x_{i_n})$. We use the Jacobi identity and the induction hypothesis. We have:

$$[x,y]\cdot P\cdot t = [x,y]\cdot x_{i_1}\cdot P'\cdot t = x_{i_1}\cdot[x,y]\cdot P\cdot t - [x_{i_1}[x,y]]\cdot P'\cdot t$$

$$= x_{i_1}\cdot x\cdot y\cdot P'\cdot t - x_{i_1}\cdot y\cdot x\cdot P'\cdot t + ([x,[y,x_{i_1}]]\cdot P' t + [y,[x_{i_1},x]]\cdot P'\cdot t)$$

$$= x_{i_1}\cdot x\cdot y\cdot P'\cdot t - x_{i_1}\cdot y\cdot x\cdot P'\cdot t - x\cdot [x_{i_1},y]\cdot P'\cdot t + [x_{i_1},y]\cdot x\cdot P'\cdot t - y\cdot [x,x_{i_1}]\cdot P'\cdot t + [x,x_{i_1}]\cdot y\cdot P'\cdot t$$

$$= (x_{i_1}\cdot x\cdot y\cdot P'\cdot t - x\cdot x_{i_1}\cdot y\cdot P'\cdot t + [x,x_{i_1}]\cdot y\cdot P'\cdot t) + (-x_{i_1}\cdot y\cdot x\cdot P'\cdot t + y\cdot x_{i_1}\cdot x\cdot P'\cdot t + [x_{i_1},y]\cdot x\cdot P'\cdot t) + (x\cdot y\cdot P\cdot t - y\cdot x\cdot P\cdot t)$$

where $P' = (x_{i_2},\ldots,x_{i_n})$.

Thus, to prove (***) we have to show that the expressions in the first two brackets are zero. But $y\cdot P\cdot t = P_2\cdot t + \sum_\alpha P_\alpha\cdot t$ where P_2 is the ordered set of elements $y,x_{i_2},\ldots,x_{i_n}$ and $l(P_\alpha) \le l(P')$. Since $x_{i_1} \ge P_2$, by (**), we get that

$$x\cdot x_{i_1}\cdot P_2\cdot t = x\cdot (x_{i_1}\cdot P_2)\cdot t = x_{i_1}\cdot x\cdot P_2\cdot t + [x,x_{i_1}]\cdot P_2\cdot t.$$

Applying the induction hypothesis $(l(P_\alpha) \le l(P') < l(P))$, we get that

$$x\cdot x_{i_1}\cdot P_\alpha\cdot t = x_{i_1}\cdot x\cdot P_\alpha\cdot t + [x,x_{i_1}]\cdot P_\alpha\cdot t.$$

Thus, the first bracket is zero. In the same way we show that the second bracket is zero. Thus, the equality (***) is proved, which completes the proof of the proposition.

q.e.d.

Remark. The module F constructed in this way is a free g–module.

Lemma I.2.1.

Let g be a Lie algebra which is generated as a k–module by the elements x_i

($i \in I$—some well-ordered index set), and let V be a cyclic g-module with generator t. Then, any element of V of the form $x_{j_1} \cdot \ldots \cdot x_{j_n} \cdot t$ is expressible as a linear combination of the elements of the form:

(*) $$x_{i_1} \cdot \ldots \cdot x_{i_m} \cdot t \text{ where } i_1 \geq \ldots \geq i_m,\ x_i \in g \text{ and } m \leq n.$$

Proof.

We carry out the proof by induction on n and for given n by induction on the number of inversions in the sequence $(x_{j_1},\ldots,x_{j_n})$. Suppose that we have already proved the lemma for $l < n$ and if $l = n$ we have proved it for the sequences $(x_{j_1},\ldots,x_{j_n})$ with $K < n_1 < n$ inversions. Then, if the sequence $(x_{j_1},\ldots,x_{j_n})$ has n_1 inversions, we write:

(**) $$x_{j_1} \cdot \ldots \cdot x_{j_n} \cdot t = x_{j_1} \cdot \ldots \cdot x_{j_{L+1}} \cdot x_{j_L} \cdot \ldots \cdot x_{j_n} \cdot t + x_{j_1} \cdot \ldots \cdot [x_{j_L}, x_{j_{L+1}}] \cdot \ldots \cdot x_{j_n} \cdot t.$$

Applying the induction hypothesis we can express the right hand side of (**) as a linear combination of the elements of the form (*).

q.e.d.

We are now in the position to prove the main theorem of this section.

Theorem I.2.1. (Birkhoff–Witt)

Let g be a Lie algebra which is free as a k-module with a k-basis $\{x_i\}_{i \in I}$ where I is some well-ordered index set. Then, if $U(g)$ is the enveloping algebra of g and $i: g \to U(g)$ is the canonical map of g into $U(g)$ (cf. Ch. I.§1), the family of elements of the form:

(*) $$i(x_{i_1}) \cdot \ldots \cdot i(x_{i_n}) \text{ with } i_1 \geq \ldots \geq i_n,\ n \geq 0$$

form a k–basis for the k–module U(g).

Proof.

Since U(g) = T(g)/I, where T(g) is a tensor algebra of g and I is the ideal of T(g) generated by the elements $[x,y] - x\otimes y + y\otimes x$ (for all $x,y\in g$), we see that the family (*) generates U(g) as a k–module (cf. Lemma I.2.1). In order to show that the family (*) is k–linearly independent, we view the g–module F constructed in Proposition I.2.1 (with $T=\{t_0\}$) as a left U(g)–module. Suppose that we have a finite linear combination of the form

$$\Sigma k_m i(x_m) = 0$$

where $k_m \in k$, $x_m = (x^m_{i_1},\dots,x^m_{i_{n(m)}})$, $i(x_m) = i(x^m_{i_1})\cdot\ldots\cdot i(x^m_{i_{n(m)}})$ and $i_1 \geq \ldots \geq i_{n(m)}$. Then, by letting this element act on t_0 we obtain

$$0 = \Sigma\, k_m i(x_m)\cdot t_0 = \Sigma\, k_m(i(x_m)t_0)$$

and hence all $k_m = 0$ since the elements $i(x_m)\cdot t_0$ form a k–basis of F, q.e.d.

We will show now some important consequences of this theorem.

Corollary I.2.1.

Let g be a Lie algebra which is free as a k–module. Then, the canonical map $i:g \longrightarrow U(g)$ is injective.

Proof.

The images of the elements of the k–basis of g under the map i form a linearly independent set.

q.e.d.

Corollary I.2.2.

Let h be a subalgebra of a Lie algebra g. Let the family $\{x_i,y_j\}_{i\in I,j\in J}$ (I,J–some well–ordered index sets) form a k–basis of g, and let the family

$\{x_i\}_{i\in I}$ be a k–basis of h. Then:

(1) The injection $h \to g \to U(g)$ can be lifted to an injection of $U(h)$ into $U(g)$.

(2) The algebra $U(g)$ is a free $U(h)$–module admitting the family

(*) $$y_{j_1}\cdot\ldots\cdot y_{j_k} \text{ with } j_1\geq\ldots\geq j_k,\ k\geq 0$$

as a basis.

Proof.

We well–order the set $I\times J$ by declaring that $i > j$ for all $i \in I$, $j \in J$. The family $\{x_{i_1}\cdot\ldots\cdot x_{i_n}\cdot y_{j_1}\cdot\ldots\cdot y_{j_m}$ with $i_1\geq\ldots\geq i_n$, $j_1\geq\ldots\geq j_m$, $n,m \geq 0\}$ is then a k–basis of the module $U(g)$. Moreover, the subfamily of the above that do not involve y's, i.e., when $m = 0$, form a k–basis of $U(h)$. This clearly implies (1) and (2).

q.e.d.

Corollary I.2.3.

Let g be a direct sum of subalgebras $g_1,\ldots,g_n$ and let g_i be a free k–module for $i = 1,2,\ldots,n$. Then, the canonical homomorphism of the k–module $U(g_1)\otimes\ldots\otimes U(g_n)$ into the k–module $U(g)$ defined by $x_1\otimes\ldots\otimes x_n \to x_1\cdot\ldots\cdot x_n$ for all $x_i \in g_i$ is a k–module isomorphism.

Proof.

Follows clearly from the Corollary I.2.2.

q.e.d.

Let g be a Lie algebra over k, and let $U(g)$ be the universal enveloping algebra of g. We define a natural filtration of $U(g)$ as follows: Let $U_n(g)$ be the submodule of $U(g)$ generated by the products $i(x_1)\cdot\ldots\cdot i(x_m)$, $m \leq n$ where $x_i \in g$. We see that

$$U_0(g) = k,\ U_1(g) = k\oplus i(g) \text{ and } U_0(g) \subset U_1(g) \subset \ldots \subset U_n(g) \subset \ldots .$$

We define $gr(U(g)) = \bigoplus_{n\geq 0} gr_n U(g)$ where $gr_n(U(g)) = U_n(g)/U_{n-1}(g)$. The map $U_m(g)\times U_n(g) \to U_{m+n}(g)$ given by $(x,y) \to x\cdot y$ for all $x \in U_m(g)$ and $y \in U_n(g)$ defines, by passage to quotient, a bilinear map

$$gr_m(U(g)) \times gr_n(U(g)) \to gr_{m+n}(U(g)).$$

Thus, we obtain a graded algebra structure on $gr(U(g))$. We call $gr(U(g))$ the graded algebra associated to $U(g)$. This algebra is associative, has a unit and is generated by the image of g in $gr(U(g))$ under the map induced by the canonical map $i:g \to U(g)$. We will now show that in fact $gr(U(g))$ is commutative. It is enough to prove that $\overline{i(x)}$ commutes with $\overline{i(y)}$ in $gr_2(U(g))$ for all $x,y \in g$. Since the canonical map i is a Lie algebra homomorphism we have $i(x)i(y) - i(y)i(x) = i([x,y])$. Since $i([x,y]) \in U_1(g)$ we see that $i(x)i(y) \equiv i(y)i(x)$ modulo $U_1(g)$. It follows that the map $g \to gr(U(g))$ can be extended to a homomorphism

$$\varphi: S(g) \to gr(U(g)).$$

where $S(g)$ is the symmetric algebra of g. Since $gr(U(g))$ is generated by the image of g, the map U is surjective. As an equivalent form of the Birkhoff–Witt theorem, we state:

<u>Corollary I.2.4.</u>

If g is a k–free module, then the map φ is injective.

<u>Proof.</u>

Let $\{x_i\}_{i\in I}$ be a k–basis of g. As before, we write $m = (i_1,\ldots,i_n)$ with $i_1\geq\ldots\geq i_n$ and $i(x_m) = i(x_{i_1})\cdot\ldots\cdot i(x_{i_n})$, and we denote the length of m by

$l(m) = n$. The image of the element $i(x_m)$ with $l(m) = n$ in $gr_n(U(g))$ is the image under the map

$\varphi: S(g) \to gr(U(g))$ of the basic monomial in $S^n(g)$. Hence, if we can show the non-existence of a relation

$$(*) \qquad \sum_{l(m)=n} k_m x_m \equiv 0 \text{ modulo } U_{n-1}(g)$$

the injectivity of φ will follow. But, the relation (*) is by Lemma I.2.1 the same as the existence of the relation

$$\sum_{l(m)=n} k_m x_m - \sum_{l(m)<n} k_m x_m = 0.$$

Such relation however contradicts that x_m's are elements of the k-basis of $U(g)$.

q.e.d.

Corollary I.2.5.

Let k be an integral domain and let g be a Lie algebra which is a free k-module. Then, $U(g)$ is an entire algebra.

Proof.

Let u and v be two non-zero elements of $U(g)$. There exist two unique natural numbers n and m such that $u \in U_n(g)$, $u \notin U_{n-1}(g)$ and $v \in U_m(g)$, $v \notin U_{m-1}(g)$. Thus, $\bar{u} = u + U_{n-1}(g)$ and $\bar{v} = v + U_{m-1}(g)$ are well-defined non-zero homogeneous elements of $gr(U(g))$. Since the algebra $gr(U(g))$ is isomorphic to the polynomial algebra $S(g)$ (Corollary I.2.4) and since the polynomial algebra over an integral domain is entire, we see that $gr(U(g))$ is entire. It follows that $\bar{u}\cdot\bar{v}$ is non-zero and homogeneous of degree $n+m$. But $\bar{u}\cdot\bar{v} = u\cdot v + U_{n+m-1}(g)$ and therefore $u\cdot v \notin U_{n+m-1}(g)$. In particular,

$u \cdot v \neq 0$. It follows that $U(g)$ is entire.

q.e.d.

---

§3 Some Results on Free Lie Algebras

The main references for this section are [3], [4], [6], [10] and [13].

Free magmas

A set M together with a map

$$M \times M \longrightarrow M$$

denoted by $(x,y) \longrightarrow xy$ is called a magma.

Let X be a set. We define inductively a family of sets $X_n (n \geq 1)$ as follows:

(1) $X_1 = X$.

(2) $X_n = \dot{\cup}\, X_p \times X_q$ where the disjoint union, $\dot{\cup}$, is taken over all $X_p \times X_q = n$ with $p+q = n$.

Put $\Gamma(X) = \dot{\cup}\, X_n$ and define $\Gamma(X) \times \Gamma(X) \longrightarrow \Gamma(X)$ by means of $X_p \times X_q \longrightarrow X_{p+q}$. The magma $\Gamma(X)$ is called the free magma on X. The elements of $\Gamma(X)$ are called monomials. There are two natural gradings of $\Gamma(X)$:

i) Total grading: $\Gamma_n(X)$ consists of all monomials v of length $l(v) = n$.

ii) Multi–grading: let Z^X be a monoid of functions from the set X into integers. For every $x \in X$ we denote by α_x the function in Z^X defined by $\alpha_x(x) = 1$ and $\alpha_x(y) = 0$ for $y \neq x$. The map $X \longrightarrow Z^X$ defined by $x \longrightarrow \alpha_x$ extends to a magma homomorphism $m : \Gamma(X) \longrightarrow Z^X$. For any

$\alpha \in Z^X$ we denote by $\Gamma_\alpha(X)$ the set of all monomials $v \in \Gamma(X)$ such that $m(v) = \alpha$. Clearly, $\Gamma_\alpha(X) \neq \phi$ if and only if the set $S_\alpha = \{x \in X | \alpha(x) \neq 0\}$ is finite and for all $x \in S_\alpha$ we have $\alpha(x) > 0$. The set of all such functions we denote by the letter Φ. We define:

$$\text{for any } \alpha \in \Phi \quad |\alpha| = \sum_{x \in X} \alpha(x).$$

Thus we obtain

$$\Gamma(X) = \bigcup_{n \geq 1} \Gamma_n(X), \; \Gamma(X) = \bigcup_{\alpha \in \Phi} \Gamma_\alpha(X), \; \Gamma_n(X) = \bigcup_{|\alpha|=n} \Gamma_\alpha(X).$$

Free algebra on X

By the free algebra on X over k we will understand the free k–module $A(X)$ with a k–basis which consists of the elements of $\Gamma(X)$, and with the multiplication induced by the multiplication in $\Gamma(X)$. Let $A_n(X)$ and $A_\alpha(X)$ be submodules of $A(X)$ generated by the elements of $\Gamma_n(X)$ and $\Gamma_\alpha(X)$ respectively ($\alpha \in \Phi$). Since we have:

$A_n(X) \cdot A_m(X) \subset A_{n+m}(X)$ and $A_\alpha(X) \cdot A_\beta(X) \subset A_{\alpha+\beta}(X)$ $(n,m \in N, \alpha,\beta \in \Phi)$

we see that $A(X)$ has two natural gradings

$$A(X) = \bigoplus_{n \geq 1} A_n(X) \text{ and } A(X) = \bigoplus_{\alpha \in \Phi} A_\alpha(X).$$

If B is any k–algebra and f is a map from the set X into the algebra B, there exists unique k–algebra homomorphism $\bar{f}: A(X) \longrightarrow B$ which extends f.

Free Lie algebra on X

Let I be the two–sided ideal of $A(X)$ generated by the elements of the form:

$$u \cdot u \text{ and } Jac(u,v,w) \cdot \text{where } u,v,w \in A(X).$$

Definition I.3.1.

The quotient algebra $A(X)/I$ is called the free Lie algebra on X over k. We will often denote it by $L(X,k)$ or simply by $L(X)$.

Some of the functorial properties of free Lie algebras are the following:

(1) If f is any map from the set X into the Lie algebra g, then there exists unique Lie algebra homomorphism $\bar{f}: L(X) \to g$ which extends f.

(2) If f is any map from the set X into the set X', then there exists unique Lie algebra homomorphism $\bar{f}: L(X) \to L(X')$ such that $\bar{f}|X = f$. Consequently, if $\{X_\beta, f_\beta^\alpha\}$ is a direct system and

$X = \varinjlim X_\alpha$ then $\varinjlim L(X_\alpha) = L(X)$.

(3) If the ring K_1 is an extension of k then

$$L(X,K_1) = L(X,k) \otimes_k K_1.$$

This follows from the fact that the pair $(L(X,k)\otimes_k K_1,\ x \to x\otimes 1)$ is a solution of the same universal mapping problem (1) as the pair $(L(X,K_1),\ x \to x)$.

We will show now that the ideal I is a graded ideal of $L(X)$ endowed with the multigrading. Indeed, let I_1 be the set of $x \in A(X)$ such that every homogeneous component of x belongs to I. Clearly I_1 is an ideal and $I_1 \subset I$. Let $x \in A(X)$, $x = \sum_{\alpha\in\Phi} x_\alpha$, x_α–homogeneous. Then $x \cdot x = \Sigma x_\alpha^2 + \sum_{\alpha\neq\beta} x_\alpha x_\beta$. But, $x_\alpha^2 \in I$, $x_\alpha x_\beta + x_\beta x_\alpha = (x_\alpha + x_\beta)^2 - x_\alpha^2 - x_\beta^2 \in I$ so that $x \cdot x \in I_1$. For three elements $x = \sum_{\alpha\in\Phi} x_\alpha$, $y = \sum_{\beta\in\Phi} y_\beta$, $z = \sum_{\gamma\in\Phi} z_\gamma$ we have

$$\mathrm{Jac}(x,y,z) = \sum_{\alpha,\beta,\gamma\in\Phi} \mathrm{Jac}(x_\alpha, y_\beta, z_\gamma) \in I_1.$$

It follows that $I = I_1$ and hence we have inherited gradings for $L(X)$:

$$L(X) = \bigoplus_{n\geq 1} L_n(X),\quad L(X) = \bigoplus_{\alpha\in\Phi} L_\alpha(X).$$

Let X be a nonempty set and let $\Gamma(X)$ be a free magma on X. The subset $R = R(X)$ of the set $\Gamma(X)$ is called a <u>basic family</u> if it is totally ordered and satisfies the following three conditions:

(R.') $X \subset R$.

(R2) The element $w = u \cdot v$ is in R if and only if

i) the elements u and v are in R and $u < v$.

ii) if $v = v_1 \cdot v_2$ then $u \geq v_1$.

(R3) If u,v and $u \cdot v$ are elements of R then $u \cdot v > u$.

The elements of R will be called basic monomials.

The subset $H = H(X)$ of the set $\Gamma(X)$ is called a P. Hall family if it is totally ordered, and satisfies conditions (R1) and (R2) together with (H3): If $u,v \in H$ with $l(u) < l(v)$ then $u < v$. Clearly any P. Hall family is a basic family. The following example shows that we can always construct a P. Hall family in $\Gamma(X)$.

Example I.3.1.

We define the sets R_n by induction as follows: we take $R_1 = X$ and we choose a total order on R_1. Suppose that we have already defined the sets $R_1, \dots R_{n-1}$ in such a way that the conditions (R1), (R2) and (R3) hold and the set $R_1 \cup \dots \cup R_{n-1}$ is totally ordered. We define the set R_n to be the set of elements of length n which satisfy condition (R2). We choose any total order on R_n and we put $u < v$ if $u \in R_k$, $k = 1,2,\dots,n-1$, and $v \in R_n$. This completes the induction process. The set $R = \bigcup_{n \geq 1} R_n$ is totally ordered and satisfies conditions (R1), (R2) and (H3).

If R is any basic family in $\Gamma(X)$ we denote by R_n and R_α the sets $R \cap \Gamma_n(X)$ and $R \cap \Gamma_\alpha(X)$ respectively, where $n \in N$ and $\alpha \in \Phi$. To simplify the notation, we will write w instead of $\epsilon(w)$ where $\epsilon : \Gamma(X) \longrightarrow L(X)$ is the canonical map from a free magma on X into a free Lie algebra on X. The bracket $[u,v]$ will denote the image of the element $u \cdot v \in \Gamma(X)$ in $L(X)$ under the map ϵ. The k–submodule of $L(X)$ generated by the set $S \subset L(X)$ will be denoted by $k\langle S \rangle$. The length of an element $u \in \Gamma(X)$ will be denoted by $|u|$ or $l(u)$.

We want to show that any basic family R is a k–basis of the module L(X) (if we identify R with its image in L(X) under the map ϵ).

Lemma I.3.1.

Let R be any basic family in $\Gamma(X)$. Then for any $\alpha \in \Phi$, $L_\alpha(X) = k<R_\alpha>$.

Proof.

We will proceed by induction on $|\alpha|$. If $|\alpha| = 1$ then $R_\alpha = \Gamma_\alpha(X)$ and since $k<\Gamma_\alpha(X)> = L_\alpha(X)$ the result follows.. If $|\alpha| > 1$, any element of $L_\alpha(X)$ can be written as a linear combination of elements $w \in \Gamma(X)$ of the form $[u,v]$ with $u \in L_\gamma(X)$, $v \in L_\beta(X)$ and $\gamma + \beta = \alpha$. Applying the induction hypothesis we get that the elements u and v are expressible as linear combinations of basic monomials. Using distributivity of the bracket we may assume that the elements u and v are already basic monomials. Using anticommutativity we may assume that an arbitrary element of $L_\alpha(X)$ is expressible as a linear combination of the elements $w = [u,v]$ with $u \in R_\gamma$, $v \in R_\beta$, $\gamma+\beta = \alpha$ and $u < v$. We want to show that each such w is expressible as a linear combination of basic monomials w' such that $w' > u$. We will do it by induction on $|\beta|$.

If $|\beta| = 1$, then $w \in R$ and by condition (R3) $w > u$.

If $|\beta| \geq 2$, then write $v = v_1 \cdot v_2$ with $v_1, v_2 \in R$ and $v_1 < v_2$. If $u \geq v_1$ then again $w \in R$ and hence $w > u$. Suppose that $u < v_1 < v_2$. Using the Jacobi identity we can write:

$$w = [u,[v_1,v_2]] = [v_1,[u,v_2]] - [v_2,[u,v_1]].$$

If β_1 and β_2 are defined by $v_1 \in R_{\beta_1}$ and $v_2 \in R_{\beta_2}$ respectively, we see that $|\beta_1| < |\beta|$ and $|\beta_2| < |\beta|$. By the induction hypothesis both $[u,v_1]$ and $[u,v_2]$ are expressible as a linear combination of basic monomials w' such that $w' > u$. Hence w is expressible as a linear combination of elements of the form $[u',v']$ with $u',v' \in R$, $u' < v'$, $[u',v'] \in \Gamma_\alpha(X)$ and $u' > u$. Any of these elements is by repeating the same argument, either a linear combination of basic monomials w'' such that $w'' > u'$ or a linear combination of elements of the form $[u'',v'']$ with $u'',v'' \in R$, $u'' < v''$, $[u'',v''] \in \Gamma_\alpha(X)$ and $u'' > u'$. Since $\Gamma_\alpha(X)$ is a finite set, this procedure must stop. It follows that w is expressible as a linear combination of basic monomials.

q.e.d.

In Section 2 of this chapter, we showed that the universal enveloping algebra $U(L)$ of the Lie algebra L with a well-ordered generating set $X = \{x_i\}_{i \in I}$ (I–some index set) is generated over k by the family of elements of the form:

$$i(x_{i_1}) \cdot \ldots \cdot i(x_{i_n}) \text{ with } x_{i_k} \in X,\ x_{i_1} \geq \ldots \geq x_{i_n},\ n \geq 0.$$

Let $L(X)$ be a free Lie algebra over k with a free generating set X.

Let φ be the canonical map $\varphi: X \to \mathrm{Lie}(\mathrm{Ass}(X))$ where Ass(X) is a free associative algebra on X. The induced Lie algebra homomorphism $\overline{\varphi}: L(X) \to \mathrm{Lie}(\mathrm{Ass}(X))$ induces the homomorphism of associative algebras $\overline{\overline{\varphi}}: U(L(X)) \to \mathrm{Ass}(X)$.

Lemma I.3.2.

The homomorphism $\overline{\overline{\varphi}}$ is an isomorphism.

Proof.

The map $X \to U(L(X))$ defines a homomorphism Ψ from $\mathrm{Ass}(X)$ into $U(L(X))$ and it is clear that $\overline{\overline{\varphi}} \cdot \Psi = \mathrm{Id}_{\mathrm{Ass}(X)}$ and $\Psi \cdot \overline{\overline{\varphi}} = \mathrm{Id}_{U(L(X))}$.

q.e.d.

As a product of this lemma and Lemma I.3.1 we get the following result:

Corollary I.3.1.

For any $\alpha \in \Phi$ with $\alpha \neq 0$, the k–submodule $Ass_{\alpha}(X)$ is generated by the following family of elements:

(I.3.1) $w_{i_1} \cdot \ldots \cdot w_{i_n}$ where $w_{i_k} = \overline{\varphi}(u_{i_k})$, $u_{i_k} \in R$, $\Sigma \alpha_{i_k} = \alpha$

and $u_{i_1} \geq \ldots \geq u_{i_n}$ (R is any basic family in $\Gamma(X)$).

We also know that for any $\alpha \in \Phi$, the k–submodule $Ass_{\alpha}(X)$ is a free k–module with a basis consiting of elements of the form:

(I.3.2) $x_{i_1} \cdot \ldots \cdot x_{i_n}$ with $m(x_{i_1} \cdot \ldots \cdot x_{i_n}) = \alpha$ where $m : \Gamma(X) \longrightarrow Z^X$.

We will show that there is one–to–one correspondence between the elements of the form (I.3.1) and (I.3.2) by proving the following lemma:

Lemma I.3.3.

There exists one and only one way to arrange Lie brackets on the associative monomial of the form (I.3.2) to obtain a Lie element of the form (I.3.1).

Proof.

We will proceed by induction on the length of an associative monomial of the form (I.3.2). The result is obviously true for monomials of length 1. Suppoe that we have proved the lemma for monomials of length less than n. We take any associative monomial v of length n. To simplify notation we will write $v = x_1 \cdot \ldots \cdot x_n$ instead of $v = x_{i_1} \cdot \ldots \cdot x_{i_n}$.

a) existence

By the induction hypothesis we can arrange Lie brackets on $v' = x_1 \cdot \ldots \cdot x_{n-1}$ to obtain an element w of Ass(X) of the form (I.3.1), i.e., $w = w_1 \cdot \ldots \cdot w_s$ where $w_i = \overline{\varphi}(u_i)$, $u_1 \geq \ldots \geq u_s$, $u_i \in R_{\alpha_i}$ and $\Sigma \alpha_i = \alpha' = m(v')$. If $x_n \leq u_s$ then put $w_{s+1} = \overline{\varphi}(x_n)$. The element $w_1 \cdot \ldots \cdot w_{s+1}$ is of the form (I.3.1) and is obtained by arranging Lie brackets on v.

Suppose that $x_n > u_s$ and let p be the smallest integer such that $[u_p,[\ldots,[u_s,x_n]\ldots]$ is a basic monomial in R, i.e., p is the smallest integer such that $u_p < [u_{p+1},[\ldots,[u_s,x_n]\ldots]$ holds. Put $w_p' = \overline{\varphi}([u_p,[\ldots[u_s,x_n]\ldots])$. If $p \neq 1$ then the element $w_1 \cdot \ldots \cdot w_{p-1} \cdot w_p'$ is of the form (I.3.1) and is obtained by arranging Lie brackets on v. If $p = 1$ then take w_1' which is of the form (I.3.1) too. It proves the existence of bracket arrangment for monomials of length n.

b) <u>uniqueness</u>

Suppose that we can arrange Lie brackets on $v = x_1 \cdot \ldots \cdot x_n$ in two ways to obtain two elements $w_1 \cdot \ldots \cdot w_s$ and $w_1' \cdot \ldots \cdot w_r'$ of the form (I.3.1).

We can write:

$u_s = [a_1,[a_2,[\ldots[a_i,x_n]\ldots]$ where $w_s = \overline{\varphi}(u_s)$, $a_j \in R$ and $a_1 \geq a_2 \geq \ldots \geq a_i$

and

$u_r' = [b_1,[b_2,[\ldots[b_m,x_n]\ldots]$ where $w_r' = \overline{\varphi}(u_r')$, $b_j \in R$ and $b_1 \geq b_2 \geq \ldots \geq b_m$.

If $w_{s-1} = \overline{\varphi}(u_{s-1})$ and $w_{r-1}' = \overline{\varphi}(u_{r-1}')$ then $u_{s-1} \geq u_s \geq a_1$ and $u_{r-1}' \geq u_r' \geq b_1$.

Hence the elements $w_1 \cdot \ldots \cdot w_{s-1} \cdot \overline{\varphi}(a_1) \cdot \ldots \cdot \varphi(a_i)$ and $w_r' \cdot \ldots \cdot w_{r-1}' \cdot \overline{\varphi}(b_1) \cdot \ldots \cdot \overline{\varphi}(b_m)$ are of the form (I.3.1) and they are obtained by arranging Lie brackets on $v' = x_1 \cdot \ldots \cdot x_{n-1}$. Applying the induction hypothesis we get that

$$s + i = r + m \quad \text{and} \quad \omega_1 = w_1 = w_1', \; \omega_{s+i-1} = \overline{\varphi}(a_i) = \overline{\varphi}(b_m).$$

Since s is the smallest integer such that the element $[\omega_s,[\omega_{s+1},[\ldots[\omega_{s+i-1},x_n]\ldots]$ is a basic monomial and since r is the smallest integer such that the element $[\omega_r,[\omega_{r+1},[\ldots[\omega_{s+i-1},x_n]\ldots]$ is a basic monomial we see that $s = r$ and $i = m$. It follows that $w_i = w_i'$ for $i = 1,2,\ldots,s$. This proves the uniqueness of bracket arrangement for monomials of length n. The lemma follows now by induction.

q.e.d.

We are now in position to prove the main theorem of this section.

<u>Theorem I.3.1.</u>

Let $L(X)$ be a free Lie algebra on X over k. Let $\overline{\varphi}: L(X) \longrightarrow \mathrm{Lie}(\mathrm{Ass}(X))$ and $\overline{\overline{\varphi}}: U(L(X)) \longrightarrow \mathrm{Ass}(X)$ be the homomorphisms induced by the map $X \longrightarrow \mathrm{Ass}(X)$. <u>Then</u>:

(1) The homomorphism $\overline{\overline{\varphi}}$ is an isomorphism.

(2) The homomorphism $\overline{\varphi}$ is an isomorphism of $L(X)$ onto the Lie subalgebra of $\mathrm{Lie}(\mathrm{Ass}(X))$ generated by X.

(3) If R is any basic family in $\Gamma(X)$ then $R_\alpha = R \cap \Gamma_\alpha(X)$ is a k–basis of $L_\alpha(X)$ for all $\alpha \in \Phi$. In other words

$$L_\alpha(X),\ L_n(X) = \bigoplus_{|\alpha|=n} L_\alpha(X) \text{ and } L(X) = \bigoplus_{n\geq 1} L_n(X)$$

are free k–modules.

(4) If X is a finite set of cardinality d then $L_n(X)$ is a free k–module of rank $l_d(n)$ and

$$\text{(I.3.3)} \quad \sum_{m|n} m l_d(m) = d^n.$$

<u>Proof.</u> (1) has been already proved (Lemma I.3.2).

Since the homomorphism $\overline{\varphi}$ maps $L(X)$ onto the Lie subalgebra of $\mathrm{Ass}(X)$ generated by X, in order to prove (2) we only have to show that $\overline{\varphi}$ is injective. If we prove (3) then by Birkhoff–Witt theorem the homomorphism $L(X) \longrightarrow U(L(X))$ will be injective. Since we can identify $U(L(X))$ with $\mathrm{Ass}(X)$

by part (1) of this theorem, (2) will follow.

Proof of (3)

In $Ass_\alpha(X)$ there exists a k–basis which consists of elements of the form (I.3.2) and a generating set which consists of elements of the form (I.3.1). By Lemma I.3.3 the numbers of elements of this k–basis and this generating set are equal. Let us denote by $A = (a_1,\dots,a_p)$ the vector of all elements of the form (I.3.2) in $Ass_\alpha(X)$ and let us denote by $B = (b_1,\dots b_p)$ the vector of all elements of the form (I.3.1) in $Ass_\alpha(X)$. Since the set $\{a_1,\dots,a_p\}$ is a k–basis of $Ass_\alpha(X)$ and the set $\{b_1,\dots,b_p\}$ generates $Ass_\alpha(X)$ over k, there exist two matrices T and S with coefficients in k such that:

$$B^t = T\cdot A^t \text{ and } A^t = S\cdot B^t.$$

It follows that

$$(ST - Id)\cdot A^t = 0$$

where Id denotes the unit $p\times p$ matrix. Since A^t is a k–basis we get that $S\cdot T = Id$. Let adj(T) denote the adjoint matrix of T. We have

$$T\cdot(S\cdot T)\cdot(adj(T)) = T\cdot(Id)\cdot(adj(T)) = \det(T)\cdot Id \text{ and}$$
$$(T\cdot S)\cdot(T\cdot(adj(T)) = T\cdot S\cdot\det(T).$$

Since $\det(T)\cdot\det(S) = 1$, $\det(T)$ is an unit in k. It follows that $T\cdot S = Id$.

Suppose that we have the following relation:

$$k_1\cdot b_1+\dots+k_p\cdot b_p = 0.$$

So, $(k_1,\dots,k_p)\cdot T = 0$ and hence

$$0 = (k_1,\dots,k_p)\cdot T\cdot S = (k_1,\dots,k_p).$$

Hence, $\{b_1,\dots,b_p\}$ is a k–basis of $Ass_\alpha(X)$.

It follows that all elements of Ass(X) of the form $\overline{\varphi}(u_{i_1})\cdot\dots\cdot\overline{\varphi}(u_{i_n})$ with $u_{i_j} \in R$ and $u_{i_1} \geq,\dots,\geq u_{i_n}$, are k–linearly independent. In particular, all elements

$\overline{\varphi}(u)$ where $u \in R$, are k–linearly independent.

It follows that the elements of R are k–linearly independent in L(X). Lemma I.3.1 now completes the proof of (3). Note also that injectivity of $\overline{\varphi}$ follows directly from this proof without any reference to the Birkhoff–Witt theorem.

Proof of (4)

Let R be any basic family in L(X). Let d_i denote the degree of $u_i \in R$ in L(X) where L(X) is endowed with the total grading ($i \in I$ where I–some index set). The Brikhoff–Witt theorem tells us that the family of elements $u^e = u_{i_1}^{e_{i_1}} \cdot \ldots \cdot u_{i_s}^{e_{i_s}}$ with $u_{i_1} > \ldots > u_{i_s}$ is a k–basis of $U(L(X)) = Ass(X)$. We have $d^0(u^e) = \Sigma e_{i_j} \cdot d_{i_j}$. If we denote by a(n) the rank of $Ass_n(X)$, then a(n) is equal to the number of fintie sequences of natural numbers (e_i) such that $n = \Sigma e_i d_i$.

This last statement is equivalent to say that the Euler-Poincaré series of Ass(X)

$$\chi_A = A(t) = \Sigma a(n) t^n$$

may be expressed in the form

$$A(t) = \prod_{i \in I} \frac{1}{1-t^{d_i}}.$$

To see this we write the formal idendity $\prod_{i \in I} 1/(1-t^{d_i}) = \prod_{i \in I} (1+t^{d_i}+t^{2d_i}+\ldots)$. The coefficient of t^n in the second product is precisely the number of sequences (e_i) such that $\Sigma e_i \cdot d_i = n$. Since for any positive integer m the number of factors in the product $\prod_{i \in I} 1/(1-t^{d_i})$ such that $d_i = m$ is exactly $l_d(m)$, we have

$$A(t) = \prod_{m \geq 1} 1/(1-t^m)^{l_d(m)}.$$

On the other hand, the set of monomials $x_{i_1} \cdot \ldots \cdot x_{i_n}$ is a k–basis of $Ass_n(X)$. Hence the rank $a(n)$ of $Ass_n(X)$ is equal to d^n. Therefore, we can also write

$$A(t) = \Sigma d^n t^n = 1/1-dt.$$

Hence

$$\prod_{m\geq 1} 1/(1-t^m)^{l_d(m)} = 1/(1-dt).$$

Using the formal equality $\mathrm{Log}(1/1-t) = \sum_{n=1}^{\infty} (1/n)\cdot t^n$ we see that

$$\sum_{m,k\geq 1} (1/k)\cdot l_d(m)\cdot t^{m\cdot k} = \sum_{n\geq 1} (1/n)d^n\cdot t^n.$$

Comparing coefficients for each natural number n we get

$$(1/n)\cdot d^n = \sum_{m\cdot k=n} (1/k)l_d(m).$$

It follows that

$$d^n = \sum_{m\mid n} m\cdot l_d(m)$$

which completes the proof of (4).

q.e.d.

We will now prove two results which we will refer to in Chapter II and III. We call a subset S of a free magma $\Gamma(X)$ a <u>left ideal</u> of $\Gamma(X)$ if for any element $u \in \Gamma(X)$ and any element $v \in S$ we have $u\cdot v \in S$. In an analogous way we define a <u>right ideal</u> in $\Gamma(X)$. An <u>ideal</u> in $\Gamma(X)$ is a subset S of $\Gamma(X)$ which is simultaneously a left and a right ideal. We call an element u of S <u>S–reducible</u> if it can be written as a product of two elements of S. Otherwise we call an element of S, <u>S–irreducible.</u>

<u>Lemma I.3.4.</u>

Let S be a subset of $\Gamma(X)$. Any element of S can be written as a product with some bracketing of S–irreducible elements of S.

Proof.

We will proceed by induction on the length of an element u of S.

The Lemma is clear if $l(u) = 1$.

Suppose that we have proved the lemma for all monomials u of length less than n. Let u be a monomial of length n. u is either S–irreducible or it can be written as a product $v \cdot w$ of two elements $v, w \in S$. In the later case, applying the induction hypothesis we express elements v and w as products of S–irreducible elements. The lemma follows.

q.e.d.

Proposition I.3.1.

Let S be a right ideal in $\Gamma(X)$ and let R be a basic family in $\Gamma(X)$ which satisfies the following condition: if $u \in R-S$ and $v \in R \cap S$ then $u < v$.

Let Y be the set of $R \cap S$–irreducible elements in $R \cap S$. Then the submodule $k<R \cap S>$ of a free Lie algebra $L(X)$ generated by the set $R \cap S$ is the free Lie algebra with free generating set Y.

Proof.

Let Y' be a set together with a bijective map $\beta: Y' \to Y$. The map β extends to the bijective map $\bar{\beta}$ from $\Gamma(Y')$ onto $\Gamma(Y)$. We want to construct certain basic family R' in $\Gamma(Y')$.

Put $R_1' = Y'$ and carry over the ordering of Y to Y' via β^{-1}.

Suppose that we have already constructed the sets $R_1', R_2', \dots, R_{m-1}'$ such that $\bar{\beta}(R_i') \subset R \cap S$ for $i = 1,2,\dots,m-1$. Suppose also that the set $R_1' \cup \dots \cup R_{m-1}'$ is totally ordered and that the restricted map $\bar{\beta} | R_1' \cup \dots \cup R_{m-1}'$ is order preserving.

We define R'_m to be the set of all products $u \cdot v$ with $u \in R'_n$ and $v \in R'_{m-n}$, such that: $u < v$ and if $v = v_1 \cdot v_2$ where $v_1, v_2 \in R'_1 \cup \ldots \cup R'_{m-1}$, $v_1 < v_2$, then $u \geq v_1$. We want to show that $\beta(R'_m) \subset R \cap S$.

Indeed, any element of R'_m is of the form $u \cdot v$ with $u \in R'_n$, $v \in R'_{m-n}$ and $\beta(u)$, $\beta(v) \in R \cap S$. Since S is a right ideal, we only need to show that $\beta(u) \cdot \beta(v) \in R$. We know that $\beta(u) < \beta(v)$.

If $v = v_1 \cdot v_2$, where $v_1, v_2 \in R'_1 \cup \ldots \cup R'_{m-1}$, $v_1 < v_2$, then $u \geq v_1$ and hence $\beta(u) \geq \beta(v_1)$ and $\beta(v_1) < \beta(v_2)$. It follows that in this case $\beta(u) \cdot \beta(v) \in R$. If v is $R'_1 \cup \ldots \cup R'_{m-n}$–irreducible then $v \in Y'$ and hence $\beta(v) \in Y$.

If $\beta(v)$ can be written as a product $\gamma_1 \gamma_2$ for some $\gamma_1, \gamma_2 \in R$ with $\gamma_1 < \gamma_2$, then at least one of γ_1 and γ_2 is in $R - S$ (since Y is the set of $R \cap S$–irreducible elements). Since by assumption $R - S < R \cap S$ we see that $\gamma_1 \in R - S$ and hence $\beta(u) \geq \gamma_1$. It follows that also in this case $\beta(u) \cdot \beta(v)$ is in $R \cap S$.

Hence, $\beta(R'_m) \subset R \cap S$.

We totally order the set $R'_1 \cup \ldots \cup R'_m$ by:

$$u < v \text{ if and only if } \beta(u) < \beta(v) \text{ for all } u, v \in R'_1 \cup \ldots \cup R'_m.$$

The subset $R' = \bigcup_{m \geq 1} R'_m$ of $\Gamma(Y')$ is then totally ordered and satisfies conditions (R1), (R2) and (R3); that is, it is a basic family in $\Gamma(Y')$.

By Theorem I.3.1, R' is a k–basis of $L(Y')$. Let $\bar{\beta}: L(Y') \to L(X)$ be Lie algebra homomorphism induced by $\beta: Y' \to Y$. Since $R \cap S$ is a part of the k–basis of $L(X)$ and $\bar{\beta}(R') = \beta(R) \subset R \cap S$ we see that $\bar{\beta}$ is injective.

If $w \in R \cap S$ then w can be written as a product with some bracketing of elements of Y. Hence $w \in \mathrm{Im}(\bar{\beta})$, i.e., $k < R \cap S > \subset \bar{\beta}(L(Y'))$. Since $\beta(R') \subset R \cap S$, we see that $\bar{\beta}(L(Y')) \subset k < R \cap S >$.

It follows that $k\langle R\cap S\rangle$ is a subalgebra of $L(X)$ which is isomorphic to free Lie algebra $L(Y')$.

q.e.d.

Proposition I.3.2. (Elimination Theorem)

Let $L(X)$ be a free Lie algebra on X over k. Let $X = X' \cup X''$ with $X' \cap X'' = \phi$ and $X' \neq \phi$. Then:

(1) The ideal $\mathfrak{a}$ of $L(X)$ generated by the set X' is a free Lie algebra with free generating set Y which consists of elements of the form:

(*) $$[u_{i_1},[u_{i_2},[\ldots[u_{i_n},x']\ldots.]$$

where u_{i_k} belongs to some basic family R'' in $\Gamma(X'')$, $x' \in X'$, $n \geq 0$ and $u_{i_1} \geq \ldots \geq u_{i_n}$.

(2) The k–module $L(X)$ is the direct sum of $\mathfrak{a}$ and H, where H is a subalgebra of $L(X)$ which is isomorphic to free Lie algebra $L(X'')$ on X''.

(3) $\mathfrak{a}/[\mathfrak{a},\mathfrak{a}]$ is a free $U(L(X)/\mathfrak{a})$–module with basis the images of the elements of the set X'.

Proof.

(1) We identify $\Gamma(X'')$ with its image in $\Gamma(X)$ under the map induced by the inclusion $X'' \longrightarrow X$. Let $S = \Gamma(X) - \Gamma(X'')$. Clearly, S is an ideal in $\Gamma(X)$. In order to use Proposition I.3.1 we have to construct a basic family R in $\Gamma(X)$ such that $R - S < R\cap S$.

Put $R_1 = X$, and totally order R_1 such that $R_1 - S = X'' < R_1 \cap S = X'$.

Suppose that we have already constructed the sets $R_1,\ldots,R_{m-1}$ such that the set $R^{m-1} = R_1 \cup \ldots \cup R_{m-1}$ is totally ordered, $R^{m-1} - S < R^{m-1} \cap S$ and elements of R^{m-1} satisfy conditions (R1), (R2) and (R3).

We define R_m to be the set of all products $u \cdot v$ of monomials in R^{m-1} such that $l(u \cdot v) = m$, $u < v$ and if $v = v_1 \cdot v_2$ where $v_1, v_2 \in R^{m-1}$, $v_1 < v_2$, then $u \geq v_1$. Let R''_m be the subset of R_m which consists of all products $u \cdot v$ with $u, v \in R^{m-1} - S$. We totally order R''_m and $R_m - R''_m$ and then we totally order $R^{m-1} \cup R_m$ requiring that

$$R^{m-1} - S < R''_m < R^{m-1} \cap S < R_m - R''_m.$$

The elements of $R^m = R_1 \cup \ldots \cup R_m$ satisfy conditions (R1) and (R2) by construction.

Let $u, v, u \cdot v \in R^m$. If $u \cdot v \in R^{m-1}$ then by induction hypothesis $u \cdot v > u$. Hence the condition (R3) is satisfied in this case.

If $u \cdot v \in R''_m$ then both u and v belong to $R^{m-1} - S$ and hence $u \cdot v > u$ by construction. If $u \cdot v \in R_m - R''_m$ then $u \cdot v > u$ by construction. Hence, the condition (R3) is satisfied.

Thus, the set $R = \bigcup_{m \geq 1} R^m$ is a basic family in $\Gamma(X)$ which satisfies $R - S < R \cap S$. The ideal $\mathfrak{a}$ is the direct sum of all submodules $k<\Gamma_\alpha(X)>$ such that $\alpha(X') > 0$; i.e., $\mathfrak{a} = K<S> = \oplus_{\alpha'} L<\Gamma_{\alpha'}(X)>$ with $\alpha' \in \Phi$ and $\alpha'(X') > 0$. Since by Theorem I.3.1 R_α is a k–basis of $k<\Gamma_\alpha(X)>$ we see that $k<R \cap S> = \mathfrak{a}$. By Proposition I.3.1 the ideal $\mathfrak{a}$ is a free Lie algebra over k with free generating set Y which consists of S–irreducible elements of $R \cap S$.

Let u be any S–irreducible element of $R \cap S$. We will prove by induction on the length of u that u has the form (*).

If $l(u) = 1$ then $u \in X'$.

If $l(u) > 1$ then let $u = u_1 \cdot u_2$ be the unique decomposition of u in R. The ideal S has the property that if $w \cdot v \in S$ then either w or v belongs to S. Since u is S–irreducible and $u_1 < u_2$ we see that $u_1 \in R - S$ and $u_2 \in R \cap S$. If $u_2 = u_3 \cdot u_4$ where $u_3 \cdot u_4 \in R \cap S$ then condition (R2) tells us that $u_1 \geq u_3$ contradicting that $R - S < R \cap S$. Hence, the element u_2 is S–irreducible of length less than $l(u)$. We apply the induction hypothesis to deduce that u is indeed of the form (*).

On the other hand, each of the elements of the form (*) is obviously S–irreducible. Since $R - S = R''$ is a basic family in $\Gamma(X'')$ by construction, we have completed the proof of (1).

(2) Let Y'' be a set with a bijective map $\varphi: Y'' \longrightarrow X''$. The map φ extends to a bijection $\overline{\varphi}: \Gamma(Y'') \longrightarrow \Gamma(X'')$. Let i be the inclusion $i: X'' \longrightarrow X$. Let $L(Y'')$ be a free Lie algebra on Y'' over k. The injective map $i \cdot \varphi: Y'' \longrightarrow X$ extends to the Lie algebras homomorphism $\overline{\overline{i}} \cdot \overline{\overline{\varphi}}: L(Y'') \longrightarrow L(X)$ which maps $L(Y'')$ onto the subalgebra H of $L(X)$ generated by the set X''. Like in the proof of Proposition I.3.1 we construct a basic family R_1 in $\Gamma(Y'')$ such that the restricted map $\overline{\varphi}|R_1$ sends R_1 onto $R'' = R - S$ in an order preserving way. The restricted map $\overline{\overline{i}} \cdot \overline{\overline{\varphi}}|R_1$ is a bijection from R_1 onto $R'' = R - S$. Since $R - S$ is a part of the k–basis of $L(X)$, we see that $\overline{\overline{i}} \cdot \overline{\overline{\varphi}}$ is an injection. since $H = k<\Gamma(X'')> = k<R-S>$ and $L(X) = k<R-S> \oplus k<R \cap S>$ we see that $L(X) = H \oplus \mathfrak{a}$ as k–modules.

(3) By the part (2) of this theorem $L/\mathfrak{a} = H \cong L(X'')$.

Since $R'' = R - S$ is a k–basis of H, the theorem of Birkhoff–Witt tells us that the family of monomials of the form

$$(**) \qquad u_{i_1} \cdot \ldots \cdot u_{i_n} \text{ with } n \geq 0,\ u_{i_k} \in R'' \text{ and } u_{i_1} \geq \ldots \geq u_{i_n}$$

is a k–basis of $U(L(X)/\mathfrak{a})$.

Since $\mathfrak{a}/[\mathfrak{a},\mathfrak{a}]$ is generated over k by the elements of the form (*) we see that $\mathfrak{a}/[\mathfrak{a},\mathfrak{a}]$ is generated as an $U(L(X)/\mathfrak{a})$–module by the set X'. Since any relation of the form

$u_1\bar{x}_1+\ldots+u_n\bar{x}_n = 0$ where $u_i \in U(L(X)/\mathfrak{a})$, $\bar{x}_i$ the image of $x_i \in X'$ in $\mathfrak{a}/[\mathfrak{a},\mathfrak{a}]$ would imply k–linear dependence of the elements of a k–basis of $\mathfrak{a}/[\mathfrak{a},\mathfrak{a}]$; we see that the elmeents of the set X' are $U(L(X)/\mathfrak{a})$–free.

q.e.d.

<u>Remark</u>. There is another proof of this proposition given in ([4], Chapter II, §9, Proposition 10, p. 131). We will not present it here since it is quite analogical to the one given above. However, in the course of that proof, another free generating set of $\mathfrak{a}$ was found. It consists of all elements of the form

$$[x''_{i_1},[x''_{i_2},[\ldots[x''_{i_n},x']\ldots]$$

where $x_{i_k} \in X''$ and $x' \in X'$. We will use this result to prove the following proposition.

<u>Proposition I.3.3.</u>

Let L be a free Lie algebra on X over k where $X = X' \cup X''$, $X' \cap X'' = \phi$ and $X' \neq \phi$.

Let $\mathfrak{a}$ be the ideal of L generated by the set X'. Let $\{y_i\}_{i\in I}$ (I–some index set) be the set which is a part of the free generating set of $\mathfrak{a}$ prescribed by the Elimination theorem (the version of it mentioned in the remark above).

Let τ be the ideal generated by $\{y_i\}_{i\in I}$. Then:

(1) L/τ is a free k–module.

(2) $\tau/[\tau,\tau]$ is a free $U(L//\tau)$–module on the images of $y_i (i\in I)$ in $\tau/[\tau,\tau]$.

<u>Proof.</u>

The ideal $\mathfrak{a}$ is by Elimination Theorem a free Lie algebra over k with free generating set consisting of all elements of the form:

(*) $$[x''_{i_1},[x''_{i_2},[\dots[x''_{i_n},x']\dots]$$

where $x''_{i_k} \in X''$, $x' \in X'$ and $n \geq 0$. Since the elements $y_i (i \in I)$ lie in the free generating set of $\mathfrak{a}$, we see that the elements of the form

(**) $$[x''_{i_1},[\dots[x''_{i_n},y_i]\dots] \quad \text{where } x''_{i_k} \in X''$$

belong to the family (*).

Since the family (**) generates τ as an ideal of $\mathfrak{a}$, we apply Proposition I.3.2 to get that the family of elements of the form (**) is a $U(\mathfrak{a}/\tau)$–basis of $\tau/[\tau,\tau]$. The algebras $L/\mathfrak{a}$ and $\mathfrak{a}/\tau$ are free Lie algebras by Proposition I.3.2 and as such they are free k–modules by Theorem I.3.1. Since we have an exact sequence:

$$0 \longrightarrow \mathfrak{a}/\tau \xrightarrow{\alpha} L/\tau \xrightarrow{\beta} L/\mathfrak{a} \longrightarrow 0$$

we see that L/τ is a free k–module, which proves (1).

Let H be a subalgebra of $L(X)$ isomorphic to $L(X'')$ and let H_1 be a subalgebra of L/τ generated by the images of X''. The restriction of β to H_1 is an isomorphism and hence identifying H_1 with $L/\mathfrak{a}$ we see that

$$L/\tau = \mathfrak{a}/\tau \oplus H_1$$

as k–modules. By Corollary I.2.3

$$U(\mathfrak{a}/\tau) \otimes_k U(H_1) \cong U(L/\tau)$$

as k–modules. It follows that

$$U(L/\tau) = \oplus U(\mathfrak{a}/\tau) x''_{i_1} \cdot \dots \cdot x''_{i_n}$$

where $n \geq 0$ and $x''_{i_k} \in X''$. Since $\tau/[\tau,\tau]$ is free $U(\mathfrak{a}/\tau)$–module we see that $\tau/[\tau,\tau]$ is free $U(L/\tau)$ module with basis $\{\bar{y}_i\}_{i\in I}$ where $\bar{y}_i$ is the image of y_i

in $\tau/[\tau,\tau]$.

q.e.d.

Remark. A set $\{y_i\}_{i\in I}$ which satisfies conditions (1) and (2) of this proposition is called Strongly free set or inert set ([1],[2]). We will study such sets in Chapter III.

Example I.3.2.

Let L be the free Lie algebra on $\{X_1,\dots X_N\}$ and let

1) $A = \{P_1,\dots,P_{N-1}\}$ where $P_i = [X_i,X_{i+1}]$ $i = 1,\dots,N-1$ and

2) $B = \{P_1,\dots,P_{N-1}\}$ where $P_i = [X_1,X_{i+1}]$ $i = 1,2,\dots,N-1$

be two sets. Then A and B are strongly free (cf. Loc. cit. Remark after Proposition I.3.3). To see this take $\mathfrak{a}$ to be the ideal of L generated by $\{X_1X_3,\dots X_M\}$ (M is the largest odd integer less than or equal to N) in the first case and take $\mathfrak{a}$ to be the ideal generated by X_1 in the second case. Next, apply Proposition I.3.3.

§4. Filtered groups

The main references for this section are [13], [12], [7], [8], [9], [6] and [4].

This paragraph is an introduction to Lie algebras associated to the lower central series of the groups, which we will study in Chapter III.

Commutator calculus

Let G be a group and let $x,y,z \in G$. We will use the following notations:

(1) $x^y = y^{-1}xy$.

(2) $[x,y] = x^{-1}y^{-1}xy$, $[\cdot,\cdot]$ is called the commutator of x and y.

We have the following identities (Witt–Hall):

(I.4.1) $[x,x] = 1,\ [y,x] = [x,y]^{-1},\ x^y = x[x,y],\ xy = yx^y = yx[x,y]$.

(I.4.2) $[x,yz] = [x,z]\cdot[x,y][[x,y],z] = [x,z][x,y]^z$.

(I.4.3) $[xy,z] = [x,z][[x,z],y][y,z] = [x,z]^y[y,z]$.

(I.4.4) $[x^y,[y,z]][y^z,[z,x]][z^x,[x,y]] = 1$.

(I.4.5) $[[x,y],z][[y,z],z][[z,x,y]$

$= [y,x][z,x][z,y]^x\cdot[x,y][x,z]^y\cdot[y,z]^x\cdot[x,z][z,x]^y$.

Let A,B be subgroups of a group G, and let $[A,B]$ denote the subgroup of G generated by the commutators $[x,y]$ for all $x \in A$, $y \in B$. If A and B are normal subgroups of a group G, then $[A,B]$ is again a normal subgroup of G which is contained in the intersection of A and B.

Let $x \in A$, $y \in B$, $z \in C$ where A,B,C are any three normal subgroups of G. Since $y^z \in B$, $x^y \in A$, we have from (I.4.4) that

$[z^x[x,y]] \subset [A,[B,C]]\cdot[B,[C,A]]$.

Since z^x runs through all elements of C if z does, we proved that

(I.4.6) $[C,[A,B] \subset [A,[B,C]]\cdot[B[C,A]]$.

<u>Filtration on a group</u>

<u>Definition I.4.1.</u>

By a filtration on a group we will understand a map $\omega: G \longrightarrow R_+ \cup \{+\infty\}$, satisfying the following conditions:

(1) $\omega(1) = +\infty$.

(2) $\omega(xy^{-1}) \geq \inf\{\omega(x),\omega(y)\}$.

(3) $\omega([x,y]) \geq \omega(x) + \omega(y)$.

For any real number α we define:

$$G_\alpha = \{x \in G \mid \omega(x) \geq \alpha\}$$
$$G_\alpha^+ = \{x \in G \mid \omega(x) > \alpha\}.$$

Condition (2) shows that G_α and G_α^+ are subgroups of G. If $x \in G_\alpha$ and $y \in G$, then $x^y \equiv y \pmod{G_\alpha^+}$ which follows from (3): $\omega([x,y]) \geq \alpha + \omega(y) > \alpha$. This proves that G_α is a normal subgroup of G. We see that $G_\alpha^+ = \bigcup_{\beta > \alpha} G_\beta$ which shows that G_α^+ is also a normal subgroup of G. If $\alpha < \beta$ then clearly

$$G_\beta \subset G_\alpha \text{ and } G_\beta^+ \subset G_\alpha^+.$$

For all $\alpha \geq 0$ we define $gr_\alpha(G) = G_\alpha / G_\alpha^+$. Then

<u>Proposition I.4.1.</u>

(1) $gr_\alpha(G)$ is an abelian group $(\alpha \geq 0)$.

(2) $\overline{(x^y)} = \bar{x}$ where $x \in G_\alpha$, $y \in G$ and $\bar{x}$ denotes the image of x in $gr_\alpha(G)$.

(3) The map $G_\alpha \times G_\beta \to G_{\alpha+\beta}$ defined by $(x,y) \to [x,y]$ induces a bilinear map $gr_\alpha(G) \times gr_\beta(G) \to gr_{\alpha+\beta}(G)$.

(4) the maps of (3) can be extended by linearity to the map $gr(G) \times gr(G) \to gr(G)$ where $gr(G) = \bigoplus_{\alpha \geq 0} gr_\alpha(G)$. This map defines a Lie algebra structure in $gr(G)$ (over $\mathbb{Z}$).

<u>Proof.</u>

(1) It follows from I.4.1(3).

(2) It was proven above.

(3) We have to show that the map $gr_\alpha(G) \times gr_\beta(G) \to gr_{\alpha+\beta}(G)$ is well–defined; i.e., that it does not depend on the choice of the representatives for $\bar{x} \in gr_\alpha(G)$, $\bar{y} \in gr_\beta(G)$ in G_α and G_β respectively. So let $x \in G_\alpha$, $y \in G_\beta$ and $u,v \in G_\alpha^+$. We have to show that $[xu,y] \equiv$

$[x,y] \bmod (G^+_{\alpha+\beta})$ and $[x,yv] \equiv [x,y] \bmod (G^+_{\alpha+\beta})$. We use the formulae (I.4.2) and (I.4.3) to obtain

$$\boxed{xu,y} = \boxed{x,y}^u + \boxed{u,y} = \boxed{x,y}$$

and $$\boxed{x,yv} = \boxed{x,v} + \boxed{x,y}^v = \boxed{x,y}.$$

We now have to prove that this map is bilinear. So let $x_1 \in G_\alpha$, $y_1 \in G_\beta$. Then, using the same formulae and (2) we get

$$\boxed{xx_1,y} = \boxed{x,y}^{x_1} + \boxed{x_1,y} = \boxed{x,y} + \boxed{x_1,y}$$

and $$\boxed{x,y_1y} = \boxed{x,y} + \boxed{x,y_1}^y = \boxed{x,y} + \boxed{x,y_1}$$

which proves (3).

(4) Let $u \in gr_\alpha(G)$, $v \in gr_\beta G$ and choose elements $x \in G_\alpha$, $y \in G_\beta$ such that $\bar{x} = u, \bar{y} = v$. Then we have $\boxed{x,y} = [u,v]$ where $[u,v]$ denotes the image of (u,v) under the map $gr_\alpha(G) \times gr_\beta(G) \to gr_{\alpha+\beta}(G)$.

If $u \in gr(G)$ then $u = \sum_\alpha u_\alpha$ where $u_\alpha \in gr_\alpha(G)$. Let $x_\alpha \in G_\alpha$ such that $\bar{x}_\alpha = u_\alpha$ for all α. Then, we have

$$[u_\alpha,u_\alpha] = \boxed{x_\alpha,x_\alpha} = \bar{1} = 0 \qquad \text{(by (I.4.1))}$$

and $$[u_\alpha,u_\beta] = \boxed{x_\alpha,x_\beta} = \boxed{x_\beta,x_\alpha}^{-1} = -[u_\beta,u_\alpha] \quad \text{(by (I.4.1))}.$$

It follows that $[u,u] = 0$.

We want to prove the Jacobi identity. By trilinearity of $Jac(\cdot,\cdot,\cdot)$ it is enough to consider the case $u \in gr_\alpha(G)$, $v \in gr_\beta(G)$ and $w \in gr_\gamma(G)$. Choose $x \in G_\alpha$, $y \in G_\beta$, $z \in G_\gamma$ such that $\bar{x} = u$, $\bar{y} = v$, $\bar{z} = w$. Then using (I.4.4) we have

$$Jac(u,v,w) = [x^y,[y,z]][y^z,[z,x]][z^x,[x,y]] \cdot G^+_{\alpha+\beta+\gamma} = \bar{1} = 0.$$

q.e.d.

When the filtration ω takes values in N (natural numbers) we call it an integral or <u>central</u> filtration. The central filtrations are in a one–to–one correspondence with the sequences of subgroups of G with the following properties:

(i) $G_1 = G$.

(ii) $G_{n+1} \subset G_n$.

(iii) $[G_n, G_m] \subset G_{n+m}$.

If (G_n) is such a sequence, define a filtration $\omega: G \longrightarrow \mathbb{N} \cup \{+\infty\}$ by $\omega(x) = \sup\{n \mid x \in G_n\}$. Such a family of subgroups of G is called a central series. The lower central series of a group G is the sequence of subgroups G_n $(n \geq 1)$ defined inductively by

$$G_1 = G, \; G_{n+1} = [G, G_n].$$

Clearly, the conditions (ii) and (i) are satisfied and we will prove (iii) by induction on n in the pair $[G_n, G_m]$.

If $n = 1$, then $[G, G_m] \subset G_{m+1}$ for all m by definition. Suppose that $n > 1$. Then

$$[G_n, G_m] = [[G, G_{n-1}], G_m] \subset [G, [G_{n-1}, G_m]] \cdot [G_{n-1}, [G, G_m]]$$
$$\subset [G, G_{n+m-1}] \cdot [G_{n-1}, G_{m+1}] \subset G_{n+m} \cdot G_{n+m} \subset G_{n+m}.$$

If (H_n) is any sequence of subgroups of G which satisfied (i), (ii) and (iii) then $H_n \supset G_n$ for all n. The proof of this is again by induction. If $n = 1$, then $H_1 = G_1$. If $n \geq 1$, we have $H_{n+1} \supset [H, H_n] \supset [G, G_n] = G_{n+1}$.

Now let

(*) $\quad 1 \longrightarrow R \xrightarrow{\alpha} F \xrightarrow{\beta} G \longrightarrow 1$

be an exact sequence of groups. Let (F_n) $(n \geq 1)$ be a central series of F_n. We define $G_n = \beta(F_n)$ and $R_n = \alpha^{-1}(F_n)$. Clearly (G_n) $(n \geq 1)$ and (R_n) $(n \geq 1)$ are central series of G and R respectively.

Lemma I.4.1.

The induced sequence

$$(**) \qquad 0 \longrightarrow gr(R) \xrightarrow{\bar{\alpha}} gr(F) \xrightarrow{\bar{\beta}} gr(G) \longrightarrow 0$$

is exact with $\bar{\alpha}$, $\bar{\beta}$–Lie algebra homomorphisms.

Proof.

We identify R with its image in F under the map α, and G with the quotient group F/R. The map α induces an injective homomorhism in degree n

$$\alpha_n : R \cap F_n / R \cap F_{n+1} \longrightarrow F_n/F_{n+1}.$$

The map β induces a surjective homomorphism in degree n

$$\beta_n : F_n/F_{n+1} \longrightarrow G_n/G_{n+1}.$$

The maps $\bar{\alpha}$ and $\bar{\beta}$ are defined to be $(\alpha_1, \alpha_2, ...)$ and $(\beta_1, \beta_2, ...)$ respectively. We will prove that the sequence (**) is exact. It is enough to look at the α_n and β_n. If $f_nF_{n+1} \in \ker(\beta_n)$, then $f_n = rf_{n+1}$ for some $r \in R$ and $f_{n+1} \in F_{n+1}$. It follows that $r \in R \cap F_n$ i.e. $\mathrm{Im}(\alpha_n) \supset \ker(\beta_n)$. On the other hand, if $r \in R \cap F_n$ then $\beta_n(rF_{n+1}) = rF_{n+1}R = \bar{1}$ i.e. $\mathrm{Im}(\alpha_n) \subset \ker(\beta_n)$. Clearly $\bar{\alpha}$ and $\bar{\beta}$ are Lie algebra homomorphisms since they are group homomorphisms and as such they preserve brackets.

q.e.d.

The (x,τ)–filtration of the free group F on $X = \{x_1, ..., x_N\}$

Let A be the Magnus algebra of formal power series in the noncommutative indeterminates $\{X_i\}_{i \in I}$ with coefficients in Z (I–some index set).

Lemma I.4.2.

The elements $a_i = 1 + X_i$ $(i \in I)$ are generators of a free group $F(A)$.

Proof.

We have to show that a freely reduced word in $a_{i_1},\dots,a_{i_k}$ is not 1 unless it is the empty word. Consider the word

$$w = a_{i_1}^{e_1}\cdot\dots\cdot a_{i_k}^{e_k}$$

where $e_j, i_j \in N$, $1 \le i_j \le N$ for $j = 1,\dots,k$, and $i_j \neq i_{j+1}$. It is easily shown that $a_i^n = 1 + nX_i + X_i^2 h(X_i)$ where h is a power series. Hence

$$w = (1+e_1X_{i_1}+X_{i_1}^2h_1(X_{i_1})\cdot\dots\cdot(1+e_kX_{i_k}+X_{i_k}^2h_k(X_{i_k})$$

which contains the unique monomial

$$e_1\cdot\dots\cdot e_k X_{i_1}\cdot\dots\cdot X_{i_k}$$

Since $e_i\cdot\dots\cdot e_k \neq 0$ we have $w \neq 1$.

In view of this lemma we will identify any free group on $\{x_i\}_{i\in I}$ with its image in A under the map defined by $x_i \longrightarrow 1 + X_i (i\in I)$. Hence, we can identify Z[F] with its image in A under the map induced by the bijection $F \longrightarrow F(A)$ (Z[F] denotes the group ring of F over Z). If τ_i $(i\in I)$ are positive integers we define a valuation w of A by setting

$$w(\Sigma a_{i_1,\dots,i_n}X_{i_1}\cdot\dots\cdot X_{i_n}) = \text{Inf}\{\tau_{i_1}+\dots+\tau_{i_n} : a_{i_1,\dots,i_n} \neq 0\}.$$

For any integer $n \ge 0$ let $A_n = \{u\in A : w(u)\ge n\}$. Then $A_0 = A$, $A_{n+1} \subseteq A_n$ and $A_n\cdot A_m \subset A_{n+m}$. Hence

$$gr(A) = \bigoplus_{n\ge 0} gr_n(A) \quad \text{where } gr_n(A) = A_n/A_{n+1}$$

has a natural structure of a graded ring. Let ξ_i denote the image of X_i in $gr_n(A)$ where $n = \tau_i$. We call ξ_i the initial form of X_i with respect to (A_n). We see that gr(A) is the ring of noncommutative polynomials in $\{\xi_i\}_{i\in I}$ over Z;i.e., $gr(A) \cong Ass_Z(\xi_i)_{i\in I}$. In view of the Theorem I.3.1, the Lie subalgebra of gr(A) generated by $\xi_i (i\in I)$ is the free Lie algebra over Z with the free generating set $\{\xi_i\}_{i\in I}$. We will denote it by L. For $n > 0$ we set $F_n = (1+A_n)\cap F$. Clearly we obtain a filtration (F_n) of F. We call this filtration the (x,τ)–filtration. Let gr(F) be the Lie algebra associated to this filtration. The mapping $F \longrightarrow A$ definded by $x \longmapsto x-1$ induces a Lie algebra homomorphism from gr(F) into gr(A) defined in the following way:

Let $\bar{x} \in F_n/F_{n+1}$ and choose $x \in F_n$ such that its image in F_n/F_{n+1} is $\bar{x}$. We can write x as

$$x = 1 + G_n + G_{n+1} + \ldots + \text{higher terms} \quad (G_n \in A^n = \{u\in A : w(u) = n\}.$$

Define $\eta(\bar{x}) = G_n$. Clearly η is well–defined and injective. If

$$y = 1 + H_m + H_{m+1} + \cdots + \text{higher terms}$$

then

$$[x,y] = 1 + (G_nH_m - H_mG_n) + \ldots + \text{higher terms}.$$

It follows that η is Lie algebra homomorphism from gr(F) into Lie (gr(A)). We use this injection to identify gr(F) with its image in gr(A). Hence $L \subset gr(F)$ since η sends $\overline{1+X_i}$ to $\overline{x_i} = \xi_i$ for all $i\in I$.

If we set $Z[F]_n = Z[F]\cap A_n$ then $(Z[F]_n)$ is a filtration of the group ring Z[F]. Let gr(Z[F]) be the associated graded ring. Since the image of the element $(1+X_i)-1$ in gr(A) is ξ_i we see that gr(Z[F]) is a subring of gr(A) which contains all generators ξ_i of gr(A) i.e.,

$$gr(Z[F]) = gr(A).$$

Let $T_n (n \geq 1)$ be the set of elements of the form x_i^e with $e = \pm 1$ and $\tau_i = n$, and define subsets of F inductively as follows: $S_1 = T_1$, and for $n > 1$ $S_n = T_n \cup T_n'$ where T_n' is the set of elements of the form $[x,y]^e$ with $e = \pm 1$, $x \in S_p$, $y \in S_q$ and $p+q = n$. Let $\tilde{F}_n$ be the subgroup of F generated by the sets S_k with $k \geq n$. Then $\tilde{F}_1 = \tilde{F}$ and $\tilde{F}_{n+1} \subset \tilde{F}_n$ by definition. We want to show that $[\tilde{F}_n, \tilde{F}_k] \subset \tilde{F}_{n+k}$. Using the formulae (I.4.2) and (I.4.3) we see that it is enough to look at the commutators $[x,y]$ where $x \in S_p$, $y \in S_q$ and $p \geq n$, $q \geq k$. But then $[x,y] \in S_{p+q}$; that is, $[x,y] \in \tilde{F}_{n+k}$. If $\tau_i = 1$ for all i then $(\tilde{F}_n)$ is obviously the lower central series of F. Let $\tilde{L}$ denote the Lie algebra associated to the filtration $(\tilde{F}_n)$; i.e., $\tilde{L} = gr(\tilde{F})$.

We claim that $\tilde{F}_n \subset F_n$ for all n. Indeed, $\tilde{F}_n$ is generated by the sets S_k with $k \geq n$. For those k, the elements of T_k and T'_k belong to $(1+A_k) \cap F$. Hence $\tilde{F}_n \subset (1+A_n) \cap F = F_n$. Thus, we obtain the induced map in degree n $\tilde{F}_n/\tilde{F}_n \longrightarrow F_n/F_{n+1}$ (for all n) and consequently the map $\varphi: gr(\tilde{F}) \longrightarrow gr(F)$ (which is in general not injective). Since the algebra $\tilde{L}$ is generated by $\{\tilde{\xi}_i\}_{i \in I}$ where $\tilde{\xi}_i$ is the image of x_i in $gr_n(\tilde{F})$ with $n = \tau_i$, we get the canonical surjective homomorphism $s: L \longrightarrow \tilde{L}$ which maps ξ_i to $\tilde{\xi}_i$. The composed homomorphism $\eta \cdot \varphi \cdot s$ is a Lie algebra homomorphism from L into Lie (gr(A)) prescribed by the theorem I.3.1 (ξ_i is mapped to ξ_i). and hence by the theorem of Birkhoff–Witt it is an injection. Hence, the map s is a bijection. This implies that the map φ is injective. We will prove by induction that $\tilde{F}_n = F_n$ for all n. Jf $n = 1$, then $\tilde{F}_1 = F = F_1$ by definition.

Suppose that $\tilde{F}_n = F_n$ for $n \leq k$. The induced map $\tilde{F}_k/\tilde{F}_{k+1} \longrightarrow F_k/F_{k+1}$ has kernel $F_{k+1} \cap \tilde{F}_k/\tilde{F}_{k+1}$. Applying the induction hypothesis we get that:

$$F_{k+1} \cap \tilde{F}_k/\tilde{F}_{k+1} = F_{k+1} \cap F_k/\tilde{F}_{k+1} = F_{k+1}/\tilde{F}_{k+1}.$$

But since the map φ is injective we see that $F_{k+1} = \tilde{F}_{k+1}$ and hence $L = \tilde{L}$.

Thus we have proved the following proposition:

Proposition I.4.2.

Let (F_n) be the (x,τ)–filtration of the free group F. Let $gr(F)$ be the associated Lie algebra and let ξ_i be the image of x_i in $gr_{\tau_i}(F)$. Then $gr(F)$ is a free Lie algebra over Z with a free generating set $\{\xi_i\}_{i\in I}$.

Proposition I.4.3.

Let (F_n) be the (x,τ)–filtration of the free group F. Put $[F,F]_n = [F,F] \cap F_n$, and let gr([F,F]) be the Lie algebra associated to the filtration $([F,F]_n)$ of [F,F]. Then

$$[gr(F),gr(F)] = gr([F,F]).$$

Proof.

Since we have the following exact sequence of groups

$$1 \longrightarrow [F,F] \longrightarrow F \longrightarrow F/[F,F] \longrightarrow 1$$

by Lemma I.4.1 we get the exact sequence of Lie algebras over Z:

$$0 \longrightarrow gr([F,F]) \longrightarrow gr(F) \longrightarrow gr(F/[F,F]) \longrightarrow 0.$$

Since F/[F,F] is an abelian group, the Lie algebra gr(F/[F,F]) is abelian which implies that $[gr(F),gr(F)] \subset gr([F,F])$.

The subgroup $[F,F]_n$ is generated modulo $[F,F]_{n+1}$ by the set T_n'. The Z–submodule $[gr(F),gr(F)]_n = [gr(F),gr(F)] \cap gr_n(F)$ is generated by the brackets $[F_k/F_{k+1},F_m/F_{m+1}]$ where $k+m=n$ and $k,m>0$.

The subgroup F_k is generated modulo F_{k+1} by the set S_k, and F_m is generated modulo F_{m+1} by the set S_m. It follows that $[gr(F),gr(F)]_n$ is generated by the set T_n' and it implies that $gr_n([F,F]) \subset [gr(F),gr(F)]_n$.

q.e.d.

Chapter II

Subalgebras of Free Lie Algebras

In this chapter, we try to answer the following question:
"When is a subalgebra of a free Lie algebra free?"
It is well–known that any subalgebra of a free Lie algebra over a field k is free ([14], [15]). This is not true when k is not a field but any commutative ring with unity. In fact, if we want to answer this quesiton using the techniques known so far, we have to restrict ourselves to the graded case, i.e., the subalgebra in question is a homogeneous subalgebra of a free Lie algebra L with repect to some N–grading of L. We also need to know that certain k–submodules of L are k–free. To ensure it we may assume that k is a commutative ring with unity which has the following property: any projective module over k is free. For example any principal ideal domain has this property. The ideas used in the proofs are contained in [3], [7], [14] and [15]. The letter k denotes a commutative ring with unity.

We start with an example of the homogeneous subalgebra of a free Lie algebra over $\mathbb{Z}$ which is not free.

Example II.1.

Let L be a free algebra on $X = \{x_1, x_2\}$ with natural N–grading; i.e., $d^0(x_1) = d^0(x_2) = 1$. Let H be the subalgebra of L generated by $2x_1, x_2$ and $[x_1, x_2]$. Since the generators are homogeneous elements of L, the algebra H is a homogeneous subalgebra of L. For any subset $S \subset L$, let $Z<S>$ denote the Z–submodule of L generated by the elements of S. We see that

$$H_1 = Z\langle 2x_1\rangle \oplus Z\langle x_2\rangle,\ H_2 = Z\langle [x_1,x_2]\rangle,\ [H,H]_1 = [H,H] \cap H_1 = 0$$

and $[H,H]_2 = Z\langle 2[x_1,x_2]\rangle$.

Hence $H/[H,H]$ has torsion element, namely $[x_1,x_2] + [H,H]$.

If H was free Lie algebra then $H/[H,H]$ would be a free Z–module.

It follows that H is not free.

To prove the main theorem of this chapter we will need the following lemma:

Lemma II.1.

Let $L(X)$ be a free Lie algebra with free generating set $X = \{x_i\}_{i\in I}$ (I – some index set). Let $Y = \{y_i\}_{i\in I}$ be any k–basis of a free k–module $k\langle X\rangle$ where $k\langle X\rangle$ is a submodule of $L(X)$ generated by X. Then Y is free generating set of $L(X)$.

Proof.

Let f be a k–linear automorphism of $k\langle X\rangle$ defined by $y_i \longrightarrow x_i$ for all $i\in I$.

Let g be a k–linear automorphism of $k\langle X\rangle$ defined by $x_i \longrightarrow y_i$ for all $i\in I$.

The restricted mappings $g|X$ and $f|X$ induce Lie algebra homomorphisms $\bar{g}$ and $\bar{f}$ from $L(X)$ into itself. Since

$$\bar{g}\circ\bar{f}|_{k\langle X\rangle} = \bar{g}|_{k\langle X\rangle}\circ\bar{f}|_{k\langle X\rangle} = g|_{k\langle X\rangle}\circ f|_{k\langle X\rangle} = g\circ f|_{k\langle X\rangle} = Id|_{k\langle X\rangle}$$

and

$$\bar{f}\circ\bar{g}|_{k\langle X\rangle} = \bar{f}|_{k\langle X\rangle}\circ\bar{g}|_{k\langle X\rangle} = f|_{k\langle X\rangle}\circ g|_{k\langle X\rangle} = f\circ g|_{k\langle X\rangle} = Id|_{k\langle X\rangle}$$

we see that

$$\bar{f}\circ\bar{g} = \bar{f}\circ\bar{g} = Id_{L(X)}$$

where $Id_{L(X)}$ is the identity map in $L(X)$. It follows that Y is free generating set of $L(X)$.

q.e.d.

We now prove the main theorem of this chapter.

Theorem II.1.

Let k be a commutative ring with unity which has a property that every projective k–module is free. Let L be a free, N–graded Lie algebra over k with free generating set X which is homogeneous with respect to the grading of L. Let H be a homogeneous subalgebra of L which is in addition a direct summand of L as a k–module. Then H is a free Lie algebra with some homogeneous free generating set B.

Proof.

By assumption, there exists a k–submodule F of L such that $L = F \oplus H$ as k–modules. Since L is a free k–module by Theorem I.3.1, both F and H are projective modules and hence free. We know that $L = \bigoplus_{n \geq 1} L_n$ and $H = \bigoplus_{n \geq 1} H_n$ where $H_n = H \cap L_n$. Hence, $F = L/H = \bigoplus_{n \geq 1} L_n/H_n$. Since F is a free k–module we see that each of the modules L_n/H_n is projective and hence free. Thus, there exist submodules F_n of L_n such that $L_n = F_n \oplus H_n$ for all n. Since each submodule L_n is free, both F_n and H_n are projective, hence free.

We can view H as an intersection of subalgebras H^k of L where

$$H^k = H_1 \oplus H_2 \oplus \ldots \oplus H_k \oplus L_{k+1} \oplus L_{k+2} \oplus \ldots \; .$$

Suppose that we can construct free generating sets B^k of H^k in such a way that:

(*) $$B_n^k = B_n^{k-1} \quad \text{for } n=1,2,\ldots,k-1$$

where $B_n^k = B^k \cap L_n$. We claim that $B = \bigcup_{n \geq 1} B_n^n$ is a free generating set of H.

Indeed, any element of H is contained in $H_1 \oplus H_2 \oplus \ldots \oplus H_n$ for large enough n. Hence, this element can be written as a Lie polynomial in the elements of the set $B_1^n \cup \ldots \cup B_n^n = B_1^1 \cup \ldots B_n^n$. It follows that B generates H as a Lie algebra.

Let $L(B)$ be a free Lie algebra on B over k.

We claim that the canonical surjective homomorphism $\alpha: L(B) \longrightarrow H$ is in fact an isomorphism.

To see this we totally order each of the sets B_n^n and then we totally order the set B requiring that if $v \in B_n^n$ and $u \in B_m^m$ then: if $n < m$ then $v < u$.

Using this total order of B we construct a basic family R in $\Gamma(B)$ where $\Gamma(B)$ denotes a free magma on B. Theorem I.3.1 tells us that R is a k–basis of $L(B)$. Suppose that we have a relation of the form

$$(**) \qquad k_1 \alpha(\gamma_{i_1}) + \ldots + k_n \cdot \alpha(\gamma_{i_n}) = 0$$

where $k_j \in k$, $\gamma_{i_j} \in R$ and $n \geq 1$. The elements γ_{i_j}, $(j = 1,2,\ldots,n)$; are basic monomials in $\Gamma(B)$ which belong to $\Gamma(B_1^1 \cup \ldots \cup B_m^m)$ for large enough m ($\Gamma(B_1^1 \cup \ldots \cup B_m^m)$ denotes a free magma on $B_1^1 \cup \ldots \cup B_m^m$). We totally order the set $B^m - (B_1^m \cup \ldots \cup B_m^m)$ and then, using already defined total order of $B_1^m \cup \ldots \cup B_m^m$, we totally order B^m requiring that if $u \in B_1^1 \cup \ldots \cup B_m^m$ and $v \in B^m - (B_1^m \cup \ldots \cup B_m^m)$ then $u < v$. Using this total order of B^m we construct a basic family R^m in $\Gamma(B^m)$ where $\Gamma(B^m)$ denotes a free magma on B^m.

Since H^m is a free Lie algebra on B^m, the set R^m is a k–basis of H^m.

The relation (**) shows that the elements $\alpha(\gamma_{i_1}),\ldots,\alpha(\gamma_{i_n})$, viewed as the elements of R^m are k–linearly dependent. This is a contradiction. It follows that the homomorphism α is bijective and consequently that H is a free Lie algebra on B.

Now, we want to show that we can construct free generating sets B^k of H^k which satisfy condition (*).

We can reduce this problem to the following one:

Let L be a free N–graded Lie algebra over k with some homogeneous free generating set X. Let H be a homogeneous subalgebra of L such that $H_m = L_n$ for $m \neq n$ and $L_n = F_n \oplus H_n$ for some k–module F_n. We want to construct free generating set W of H such that $W_k = X_k$ for $k < n$ where $W_n = W \cap L_n$ and $X_n = X \cap L_n$.

Let G be the homogeneous subalgebra of H generated by the set $X_1 \cup \ldots \cup X_{n-1}$. We see that $L_n = k<X_n> \oplus G_n$ as k–modules, where $k<X_n>$ is a k–submodule of L generated by X_n.

Since $G_n \subset H_n$, we see that $H_n = (k<X_n> \cap H_n) \oplus G_n$. Thus,

$$k<X_n>/k<X_n>\cap H_n \cong k<X_n>+H_n/H_n \cong k<X_n> + G_n/H_n \cong L_n/H_n \cong F_n.$$

Since the module F_n is projective, there exists a submodule M_n of L_n such that $k<X_n> = (k<X_n> \cap H_n) \oplus M_n$. Since $k<X_n>$ is a free k–module, both M_n and $k<X_n> \cap H_n$ are free k–modules.

Hence, we can choose a k–basis $Y_n = Y_n^1 \cup Y_n^2$ of $k<X_n>$ such that Y_n^1 is a k–basis of $k<X_n> \cap H_n$ and Y_n^2 is a k–basis of M_n.

Put $Y_m = X_m$ for $m \neq n$. We see that $Y = \bigcup_{m \geq 1} Y_m$ is a k–basis of $k<X>$.

Hence, Y is a free generating set of L by Lemma II.1.

Put $S = \Gamma(Y) - Y_n^2$ where $\Gamma(Y)$ is a free magma on Y. Clearly S is an ideal in $\Gamma(Y)$. We totally order the set Y requiring that $Y_n^2 < Y - Y_n^2$. Using this total order of Y we construct a basic family R in $\Gamma(Y)$. Clearly, $R - S < R \cap S$. Since $H = k<S> = k<R \cap S>$, Proposition I.3.1 tells us that H is a free Lie algebra over k with free generating set W consisting of S–irreducible elements of $R \cap S$. Since $H_n = k<Y_n^1> \oplus G_n$, we see that any S–irreducible element of $R \cap S$ of degree less than or equal to n, necessarily belongs to the set $Y_1 \cup \ldots \cup Y_{n-1} \cup Y_n^1$.

Thus H is a free Lie algebra with free generating set W such that $W_m = Y_m = X_m$ for $m < n$. It solves our problem and consequently proves the theorem.

q.e.d.

Using this theorem we will now prove two classical results ([14], [15]).

Theorem II.2. (Sirsov)

Let k be any field and let L be the free Lie algebra on X over k. Let H be any nonzero subalgebra of L. Then H is a free Lie algebra.

Proof.

We endow L with a total grading; i.e., the k–module L_n is generated by the images of elements of $\Gamma(X)$ of length n. We define a filtration $(H_n)_{n\geq 1}$ of H by setting $H_n = H \cap (L_1 \oplus \ldots \oplus L_n)$. Let gr(H) be a graded algebra associated to this filtration; i.e., $gr(H) = \bigoplus_{n\geq 1} gr_n(H)$ where $gr_n(H) = H_n/H_{n-1}$. The k–linear homomorphism α_n from H_n into L_n defined by

$$h_n = l_1 + \ldots + l_n \xrightarrow{\alpha_n} l_n$$

induces an injective homomorphism $\overline{\alpha}_n$ from H_n/H_{n-1} into L_n. Hence, the map $\overline{\alpha} = (\overline{\alpha}_1, \overline{\alpha}_2, \ldots)$ is an injective Lie algebra homomorphism from gr(H) into L_n. We will identify gr(H) with its image in L under the map $\overline{\alpha}$.

Since k is a field and gr(H) is a homogeneous subalgebra of L, Theorem II.1

tells us that gr(H) is a free Lie subalgebra of L with some homogeneous, free generating set W.

For each element $w \in W$ let $y(w)$ be an element of H_n such that $\overline{\alpha}(y(w)) = w$, where n is the degree of w in gr(H).

Put $Y = \{y(w), w \in W\}$. Obviously the map $\beta: W \longrightarrow Y$ defined by $w \longrightarrow y(w)$ is bijective. We totally order the set W and then we totally order the set Y via β; i.e, $y(w_1) < y(w_2)$ if and only if $w_1 < w_2$. Using this total order of W we construct a basic family R in $\Gamma(W)$ where $\Gamma(W)$ denotes a free magma on W. The map β induces a bijection of magmas $\overline{\beta}: \Gamma(W) \longrightarrow \Gamma(Y)$. The image of R under the map $\overline{\beta}$ is a basic family $\overline{R}$ in $\Gamma(Y)$. Let H^1 be the subalgebra of H generated by Y. The map β induces the canonical surjective homomorphism $\overline{\overline{\beta}}: gr(H) \longrightarrow H^1$. We want to show that $\overline{\overline{\beta}}$ is injective.

Suppose that we have the following relation:

(*) $$k_i \gamma_1 + \dots + k_n \gamma_n = 0$$

where $k_i \in k$ and $\gamma_i \in \epsilon(\overline{R})$ (ϵ is the canonical map $\Gamma(Y) \longrightarrow H^1$) for $i = 1,2,\dots,n$. Let $\omega(\gamma_i) = \sup\{n \mid \gamma_i \in H_n\}$ and let $N = \mathrm{Sup}\{\omega(\gamma_i), i = 1,2,\dots,n\}$. Let S be the set $\{\gamma_i : \omega(\gamma_i) = N\}$.

The relation (*) induces k–linear relation of the highest components of the elements $\gamma_{i_k} \in S$. Since those highest components are elements of R, they are k–linearly independent by Theorem I.3.1. It follows that all the coefficients k_{i_k} are zero. We repeat this argument with reduced relation

$$k_{j_1} \gamma_{j_1} + \dots + k_{j_m} \gamma_{j_m} = 0$$

where $k_{j_i} \in k$ and $\gamma_{j_i} \in \epsilon(\overline{R}) - S$ for $i=1,2,\dots,m$.

It follows that all the coefficients k_i are zero ($i=1,2,\dots,n$) and hence that the map $\overline{\beta}$ is bijective.

We will now show that $H^1 = H$.

Let h be any element of H. There exists unique natural number n such that $h \in H_n$ but $h \notin H_{n-1}$. Let l_n be the highest component of h. We can write l_n as a linear combination of elements of the basic family R:

$$l_n = k_1 x_1 + \ldots + k_m x_m$$

where $k_i \in k$ and $x_i \in R$. There exists an element h_n of H^1 which has the same highest component as the element h, namely

$$h_n = k_1 \overline{\beta}(x_1) + \ldots + k_m \overline{\beta}(x_m).$$

To see this, note that the isomorphism $\overline{\beta}^{-1}$ maps any element of H^1 to its highest component. Thus, $h - h_n \in H_{n-1}$. If we repeat the above argument to the element $h - h_n$ instead of h, we will find an element $h_{n-1} \in H^1$ such that $h - h_n - h_{n-1} \in H_{n-2}$. This procedure must stop. Hence, we can find the elements $h_1, \ldots, h_n$ of H^1 such that $h = h_1 + \ldots + h_n$.

It follows that $H = H^1$ and it proves our theorem.

q.e.d.

<u>Theorem II.3.</u> (Witt)

Let L be a free, N–graded Lie algebra over a principal ideal domain k. Let H be a homogeneous subalgebra of L. If the quotient module L/H is free, then H is a free Lie algebra over k.

<u>Proof.</u>

It suffices to notice that H is a direct summand of L. The theorem follows now from Theorem 2.1.

q.e.d.

There is another way to obtain the similar result to Theorem 2.1 which we will present now. The main references for this section are [5], [7] and the end of Section 1 in Chapter I. The letter k denotes a commutative ring with unity with a property that any projective k–module is free.

Let L and H be N–graded Lie algebras over k and let $f:H \longrightarrow L$ be a graded Lie algebra homomorphism. Let $\bar{f}:H/[H,H] \longrightarrow L/[L,L]$ be a homomorphism induced by f. We will need the following lemmas:

<u>Lemma II.2.</u>

The homomorphism f is surjective if and only if the induced homomorphism $\bar{f}$ is surjective. In particular, if f is injective and $\bar{f}$ is surjective, then f is bijective.

<u>Proof.</u>

If f is is surjective, then obviously $\bar{f}$ is surjective.

Suppose that $\bar{f}$ is surjective. We will show by induction on the degrees that f is surjective. In degree one $f = \bar{f}$. Suppose that f is surjective in degrees less than n. Let x be a homogenous element of L_n. By surjectivity of $\bar{f}$, there exists an element y of H_n such that $x \equiv f(y) \mathrm{mod}([L,L]_n = [L,L] \cap L_n)$. But since $[L,L]_n$ is generated by elements of the form $[a,b]$ where $a \in L_p$, $b \in L_q$ and $p+q = n$, we see that we can express x as

$$x = f(y) + \sum_i [f(w_i), f(z_i)]$$

for some elements $w_i \in H_{p(i)}$, $z_i \in H_{q(i)}$ with $p(i) + q(i) = n$.

It follows that f is surjective in degree n.

q.e.d.

Lemma II.3.

If the algebra L is a free k–module, and if $H_2(L,k) = 0$ (cf. Loc. cit. Ch. I§.1) then the homomorphism f is bijective if and only if the algebra H is a free k–module and the induced homomorphism $\bar{f}$ is bijective.

Proof.

If f is a bijective homomorphism, then obviously the induced homomorphism $\bar{f}$ is bijective and H is a free k–module.

If $\bar{f}$ is surjective then by Lemma II.2 f is surjective. Hence,

$$0 \to R \to H \xrightarrow{f} L \to 0 \quad \text{where } R = \ker(f)$$

is an exact sequence of Lie algebras. Since L is a free k–module, this exact sequence splits. It follows that R is a free k–module. Hence, we can use the Hochschild–Serre sequence (cf. Loc. cit. Ch. I§.1 and [5]) to obtain an exact sequence.

$$(*) \qquad H_2(L,k) \to H_0(L,H_1(R,k)) \to H_1(H,k) \to H_1(L,k) \to 0.$$

We have shown in Chapter I§.1, that we can identify $H_0(g,V)$ with $V/V\cdot g$ where g is a Lie algebra, V is any right g–module.

We have also shown that if g operates trivially on V then $H_1(g,V)$ is isomorphic to $V \otimes_k g/[g,g]$. Since by assumption $H_2(L,k) = 0$, we can rewrite the sequence (*) in the form

$$0 \to (R/[R,R])/(R/[R,R])\cdot L \to H/[H,H] \xrightarrow{\bar{f}} L/[L,L] \to 0.$$

The action of L on R is induced by the action of H on R, i.e, by the adjoint representation. Thus

$$(R/[R,R])/(R/[R,R])\cdot L \cong (R/[R,R])/(R\cdot H/[R,R] \cong R/R\cdot H = R/[R,H].$$

Since $\bar{f}$ is injective we see that $R/[R,H] = 0$. We will show that this implies that $R = 0$. Indeed, the ideal R is a graded ideal with grading induced by that of H. Let n be the smallest integer such that $R_n \neq 0$ (n is necessarily greater than 1). Since $R_n/[R,R]_n = 0$ we see that R_n is generated by elements of the form $[a,b]$ where $a \in R_p$, $b \in R_q$ and $p+q = n$. Since $R_m = 0$ for $m < n$ we see that $R_n = 0$. It follows that f is bijective.

q.e.d.

Lemma II.4.

Let L be N–graded Lie algebra. Then L is a free Lie algebra if and only if:

(1) L is a free k–module.

(2) $L/[L,L]$ is a free k–module.

(3) $H_2(L,k) = 0$.

Proof.

Suppose that L is a free Lie algebra with free generating set $X = \{x_i\}_{i \in I}$ (I – some index set). By Theorem I.3.1 L is a free k–module. Let $\bar{x}_i$ be the image of x_i in $L/[L,L]$. Then obviously $L/[L,L]$ is a free k–module with basis $\{\bar{x}_i\}_{i \in I}$.

Let ϵ be augmentation map from U(L) onto k and let $I = \ker(\epsilon)$ be the augmentation ideal of U(L). The algebra U(L) is by Theorem I.3.1 the free associative algebra on X.

Hence, the ideal I is a direct sum of submodules $U(L) \cdot x_i$ ($i \in I$). It follows that the exact sequence

(*) $$0 \longrightarrow I \hookrightarrow U(L) \xrightarrow{\epsilon} k \longrightarrow 0$$

is a k–resolution of free U(L)–modules. Hence, $H_2(L,V) = 0$ for all right L–modules V. Suppose now that conditions (1), (2) and (3) hold.

Since $L/[L,L] = \bigoplus_{n\geq 1}(L/[L,L])_n$, we see that each submodule $(L/[L,L])_n$ is projective and hence free. It follows that we can choose a homogeneous k–basis $\bar{Y} = \{\bar{y}_j\}_{j\in J}$ of $L/[L,L]$ (J – some index set). Let y_i be a homogeneous element of L whose image in $L/[L,L]$ is $\bar{y}_i$. Let H be the subalgebra of L generated by $Y = \{y_j\}_{j\in J}$. The inclusion $\varphi: H \to L$ induces the surjective homomorphism $\bar{\varphi}: H/[H,H] \to L/[L,L]$. By Lemma II.2 the map φ is surjective. Thus L is generated by Y.

Let L(Y) be a free Lie algebra on Y over k. L(Y) has natural N–grading structure induced by degrees of the elements $y_j (j\in J)$. Let $\beta: L(Y) \to L$ be the canonical surjection. Since the set $\bar{Y}$ is a k–basis of $L/[L,L]$ we see that the induced homomorphism $\bar{\beta}: L(Y)/[L(Y),L(Y)] \to L/[L,L]$ is bijective. Since L(Y) is a free

k–module, Lemma II.3 tells us that β is bijective. Thus, L is a free Lie algebra.

q.e.d.

We are now in the position to prove the following proposition.

<u>Proposition II.1.</u>

Let L be a free, N–graded Lie algebra and let H be a homogeneous subalgebra of L. If L/H and H/[H,H] are free k–modules then H is a free Lie algebra.

<u>Proof.</u>

Since L/H is a free k–module we see that $L \cong H \oplus L/H$ as k–modules. Since L is a free k–module by Theorem I.3.1 we see that H is projective, hence free. Let U(L) and U(H) be the universal enveloping algebras of L and H respectively. By Corollary I.2.2 the algebra U(L) is a free U(H)–module. Let I be the augmentation ideal of U(L). Since $I = \bigoplus_{i\in I} U(L)x_i$ where $x = \{x_i\}_{i\in I}$

is a free generating set of L, we see that I is a free U(H)–module. Hence, the exact sequence

$$0 \longrightarrow I \longrightarrow U(L) \xrightarrow{\varepsilon} k \longrightarrow 0$$

is a k–resolution of free U(H)–modules. It follows that $H_2(H,V) = 0$ for all right H–modules V. Thus, we can apply Lemma II.4 to the algebra H to get that H is a free Lie algebra.

q.e.d.

Remark. This result is weaker than Theorem II.1 since we need to assume that H/[H,H] is a free k–module. The following example shows that we cannot conclude that H/[H,H] is a free k–module assuming only that H is a free k–module.

Example II.2.

Let L be a Lie algebra over the integers, generated by $x = \{x_1,x_2,x_3\}$ with the single defining relation $2x_1 = [x_2,x_3]$ and the degrees of x_1,x_2 and x_3 are equal to 2, 1 and 1 respectively. We need some results from Chapter III to show that L is in fact a free abelian group. Assuming this for the moment we see that L/[L,L] cannot be free Z–module since it has torsion element $\bar{x}_1$.
We will return to this example in Example III.3 in Chapter III.

Chapter III.

Lie algebras associated to the lower central series of a group

The main purpose of this chapter is to determine the Lie algebra associated to the lower central series of a finitely presented group in the case where the defining relators satisfy certain independence conditions. The methods apply to other central series such as the lower p–central series of a group. However, the proofs are entirely analogous to the ones given below, so we will only refer the interested reader to the literature. The main references for this chapter are [1], [2], [7], [8], [9], [10], [11] [12] and [13]. For the reader interested in p–central series, the main references are [22], [10] and [9]. The reader interested in the applications of this theory to link groups is refered to [1], [23], [24], [25], [26] and [27]. Some results presented here may be also obtained by using other methods. The interested reader is refered to [18] and [19].

The introductory material for this chapter is contained in Chapter I.

Let F be a free group on N–letters $x_1,\dots,x_N$ and let (F_n) be the (x,τ) filtration of F. Let ξ_i be the images of x_i in $gr_n(F)$ where $n=\tau_i$, $i=1,2,\dots,N$ and $gr_n(F)=F_n/F_{n+1}$ $(n\geq 1)$. The Lie algebra $L=gr(F)$ associated to the filtration (F_n) is by Proposition I.4.2 a free Lie algebra with free generating set $\{\xi_1,\dots,\xi_N\}$. If $x\in F$, $x\neq 1$, there is a largest integer $n=\omega(x)\geq 1$ such that $x\in F_n$. This integer is called the height of x with respect to (F_n). The image of x in $gr_{\omega(x)}(F)$ is called the initial form of x with respect to (F_n) (We will write inn(x) for initial form of x.). If $x=1$, its initial form is defined to be zero. Let $r_1,\dots r_t$ be any elements of F, and let $R=(r_1,\dots,r_t)$ be the normal subgroup of F generated by the elements r_i, $i=1,\dots,t$. Let $\rho_i=\mathrm{inn}(r_i)$ be the initial form of r_i for $i=1,2,\dots,t$; and let $\tau=(\rho_1,\dots,\rho_t)$ be the ideal of L generated by ρ_i $i=1,2,\dots,t$. Let $U(L/\tau)$ be the universal enveloping algebra of L/τ. Then $\tau/[\tau,\tau]$ becomes a

$U(L/\tau)$–module via the adjoint representation (cf. Loc. cit. Ch.I), where $[\tau,\tau]$ denotes, as usual, the derived algebra of τ. Let (G_n) and (R_n) be induced filtrations of $G = F/R$ and R respectively i.e., $G_n = F_n \cdot R/R$ and $R_n = R \cap F_n$. If g denotes the Lie algebra $gr(G)$ associated to the filtration (G_n) of G we have (by Proposition I.4.1) the exact sequence of Lie algebras:

$$0 \to gr(R) \to L \to g \to 0.$$

If we identify $gr(R)$ with its image in L, then clearly $\tau \subset gr(R)$. The natural question which arises here is: "when is τ equal to

gr(R)?" The example below shows that this is not a "trivial" question.

<u>Example III.1.</u>

Let $F = F(x_1,x_2)$ be a free group with two generators x_1 and x_2 of degree 1 i.e, $\tau_1 = \tau_2 = 1$. Let $r_1 = x_1^2$ be a relator and let $R = (r_1)$ be the normal subgroup of F generated by r_1. Using the formula (I.4.2) we get

$$[x_2,x_1^2] = [x_2,x_1]^2 \cdot [[x_2,x_1],x_1] \text{ and}$$

$$(*) \qquad [[x_2,x_1],[x_2,x_1^2]]$$
$$= [[x_2,x_1],[[x_2,x_1],x_1]] \cdot [[x_2,x_1],$$
$$[x_2,x_1]^2] \cdot [[[x_2,x_1],[x_2,x_1]^2],[[x_2,x_1],x_1]].$$

Denote the images of three factors on the right hand side of (*) by a,b,c respectively. It follows that $\omega(a) = 5$, $\omega(b) = 4$ and $\omega(c) = 7$. Hence, the element

$$a = [[\xi_2,\xi_1],[[\xi_2,\xi_1],\xi_1]]$$

is a nonzero homogeneous element of $gr_5(R)$. We will show that this element does not belong to τ where τ is the ideal of $L = gr(F)$ generated by $2\xi_1$. Since $gr(F)$ is a free Z–module, τ is free (as a submodule of $gr(F)$). Let $\{\gamma_i\}_{i\in I}$ be its Z–basis (I–some index set). We can write $\gamma_i = 2\gamma_i'$ for some

$\gamma_i' \in L(i \in I)$. We choose an order $\xi_2 < \xi_1$ and we construct the Hall basis induced by this order (cf. Loc. cit. Ch. I§.3, Example I.3.1). It follows that element a satisfies conditions R1, R2 and R3, i.e., it belongs to some Z–basis of L. Let $\{\eta_\alpha\}_{\alpha \in J}$ be elements of this basis ($\alpha \in J$; J – some index set). If $a \in \tau$, then we could write

$$a = n_1\gamma_{i_1} + \ldots + n_k\gamma_{i_k} = 2n_1\gamma'_{i_1} + \ldots + 2n_k\gamma'_{i_k} \quad (n_i \in Z,\ i=1,2,\ldots,k).$$

Since we can write

$$\gamma'_{i_j} = m_{i_1}\eta_{\alpha_1} + \ldots + m_{i_M}\eta_{\alpha_M} \quad (m_{i_p} \in Z,\ i = 1,2,\ldots,k;\ p = 1,2,\ldots,M).$$

We see that

$$a = (2n_1m_{1_1} + \ldots + 2n_km_{k_1})\eta_{\alpha_1} + \ldots + (2n_1m_{1_M} + \ldots + 2n_km_{k_M})\eta_{\alpha_M}.$$

It follows that there exists a natural number $g \in \{1,2,\ldots,M\}$ such that $a = \eta_{\alpha_q}$.

Therefore, we can write

$$1 = 2n_1m_{1_q} + \ldots + 2n_km_{k_q}$$

which is impossible. Thus, a does not belong to τ.

We will partially answer the question stated above by proving the following theorem:

Theorem III.1.

If (1) L/τ is a free Z–module, and

(2) $\tau/[\tau,\tau]$ is a free $U(L/\tau)$–module on the images of $\rho_1,\ldots,\rho_t$ then $g = L/\tau$.

Proof.

Using Lemma II.2 we see that $\tau = gr(R)$ if and only if the homomorphism

$$\tilde{\theta}: \tau/[\tau,\tau] \to gr(R)/[gr(R),gr(R)]$$

induced by inclusion $\tau \longrightarrow gr(R)$ is surjective (and hence bijective).

Using formula I.1.3 we get the canonical surjective homomorphism

$$\psi: U(L/\tau) \longrightarrow U(L/gr(R))$$

induced by surjection $L/\tau \longrightarrow L/gr(R)$.

We claim that ψ is compatible with θ in the sense that $\theta(u \cdot x) = \psi(u) \cdot \theta(x)$ for all $x \in \tau/[\tau,\tau]$, $u \in U(L/\tau)$. It is enough to show this for generators. So if $y \in L$ and $x \in \tau$, then $y\tau$ acts on $x[\tau,\tau]$ via the adjoint representation i.e., $y\tau \cdot x[\tau,\tau] = [y,x][\tau,\tau]$. Now $\psi(y\tau) = ygr(R)$, $\theta(x[\tau,\tau]) = x[gr(R),gr(R)]$ and $\theta([y,x][\tau,\tau]) = [y,x][gr(R),gr(R)]$, and since $ygr(R) \cdot x[gr(R),gr(R)] = [y,x][gr(R),gr(R)]$ we see that indeed $\theta(y\tau \cdot x[\tau,\tau]) = \psi(y\tau) \cdot \theta(x[\tau,\tau])$.

Let $M = R/[R,R]$ and let M_n be the image of R_n in M. In view of Lemma I.4.1 we have an isomorphism $gr(M) = gr(R)/gr([R,R])$ where $gr([R,R])$ is the Lie algebra associated to the filtration $([R,R]_n)$ of $[R,R]$ with $[R,R] \cap F_n = [R,R]_n$.

Since the commutator in M is trivial, $gr(M)$ is an abelian Lie algebra. Thus, we obtain the canonical surjective homomorphism

$$\theta' : gr(R)/[gr(R),gr(R)] \longrightarrow gr(M).$$

We need the following result:

Let k be a commutative ring with unity. If we have the exact sequence of groups

$$1 \longrightarrow R \xrightarrow{\alpha} F \xrightarrow{\beta} F/R \longrightarrow 1$$

then we obtain the following exact sequence of rings

$$0 \longrightarrow I(R) \xrightarrow{\overline{\alpha}} k[F] \xrightarrow{\overline{\beta}} k[F/R] \longrightarrow 0$$

where $k[F]$ and $k[F/R]$ denote the group rings of F and F/R respectively, and $I(R)$ is the ideal of $k[F]$ generated by $r-1$ for all $r \in R$.

In order to prove this, suppose that we have a relation

$$\sum_{i=1}^{n} k_i\bar{f}_i = 0 \text{ where } k_i \in k,\ f_i \in F,\ \bar{f}_i = f_iR,\ i = 1,2,\dots,n.$$

Let $f_{i_1}, f_{i_2}, \dots, f_{i_m}$ be all of f_i's such that $f_{i_1}R = f_{i_2}R = \dots = f_{i_m}\cdot R$. It follows that $k_{i_1} + \dots + k_{i_m} = 0$ and $f_{i_2} = f_{i_1}\cdot r_2, \dots, f_{i_m} = f_{i_1}\cdot r_m$ for some $r_2, \dots, r_m \in R$. Thus, we can write

$$\sum_{j=1}^{m} k_{i_j}\cdot f_{i_j} = \sum_{j=2}^{m} k_{i_j}\cdot f_{i_1}\cdot r_j + k_{i_1}\cdot f_{i_1} = f_{i_1}\cdot \sum_{j=2}^{m} k_{i_j}\cdot (r_j - 1).$$

q.e.d.

In view of this result, let $(Z[G]_n)$ and $(I(R)_n)$ denote the filtrations of $Z[G]$ and $I(R)$ respectively induced by the filtration $(Z[F]_n)$ of $Z[F]$ (cf. Loc. cit. Ch.I§.4). Let $gr(Z[G])$ and $gr(I(R))$ be graded rings associated to the filtrations $(Z[G]_n)$ and $(I(R)_n)$ respectively. The mapping from F into the Magnus algebra A (cf. Loc. cit. Ch. I§.4) defined by $x \longrightarrow x-1$ maps R into $I(R)$, hence the induced injection $\eta: gr(F) \longrightarrow gr(A)$ (cf. Loc. cit. Ch.I§.4) maps $gr(R)$ into $gr(I(R))$. Since the kernel K of the canonical map $U(L) \longrightarrow U(L/gr(R))$ is generated by the image of $gr(R)$ in $U(L)$ under the map η (by I.1.3), we get the inclusion $K \subset gr(I(R))$. Thus, we obtain the induced surjective homomorphism

$$\psi': U(L/gr(R)) \longrightarrow gr(Z[G]) \quad (\overline{x_i - 1}\cdot K \longrightarrow \overline{y_i - 1} \text{ where } y_i = x_iR).$$

We want to show that $gr(M)$ is a $gr(Z[G])$ module.

The group G acts on M. The action is induced by the action of F on R via the inner automorphisms i.e, for $x \in F$ and $v \in R$ $xR\cdot v[R,R] = xvx^{-1}[R,R]$. Since M is an abelian group, M becomes a $Z[G]$ module and $(xR-1)\cdot v[R,R] = xvx^{-1}v^{-1}[R,R]$. Let $\epsilon: A \longrightarrow Z$ be augmented homomorphism defined by

$X_i \to 0$.

The restriction of ϵ to Z[F] maps $\sum_i n_i f_i$ to $\sum_i n_i$ ($n_i \in Z$, $f_i \in F$ $i = 1,2,\ldots,n$), so it is the map induced by the homomorphism $F \to 1$. Hence, the kernel of this map is the ideal I(F) generated by $x-1$ for all $x \in F$. Let J_n be the image of $I(F)_n$ under the canonical map $Z[F] \to Z[G]$. It follows that $J_n \cdot M_k \subset M_{n+k}$ and hence $Z[G]_n \cdot M_k \subset M_{n+k}$. Thus gr(M) becomes a graded gr(Z[G]) module.

We want to show that θ' is compatible with ψ' in the sense that $\theta'(u \cdot x) = \psi'(u) \cdot \theta'(x)$ for all $u \in U(L/gr(R))$ and $x \in gr(R)/[gr(R),gr(R)]$. It is sufficient to show it for generators. So, let $\bar{r}_n \in gr_n(R)$ be a homogeneous element of gr(R) and let r_n be its representative in R_n. Then,

$\theta'(\xi_i \cdot K \cdot \bar{r}_n[gr(R),gr(R)]) =$

$\theta'(\overline{x_i - 1}K \cdot \bar{r}_n[gr(R),gr(R)]) = \theta'(\boxed{x_i,r_n}[gr(R),gr(R)]) = \boxed{x_i,r_n}gr([R,R])$ where $\overline{x_i - 1} = \xi_i$ is the image of $x_i - 1$ in gr(Z[F]) and $\boxed{x_i,r_n}$ is the image of $[x_i,r_n]$ in gr(R). But, $\boxed{x_i,r_n}gr([R,R]) = \overline{y_i - 1} \cdot r_n gr([R,R]) = \psi'(\xi_i K) \cdot \theta'(\bar{r}_n[gr(R),gr(R)])$.

q.e.d.

We want to show that the homomorphisms θ and θ' are bijective. The proof is by induction on the degrees. For $d^o = 1$, this is obviously true. Suppose that θ and θ' are bijective in degrees $n < k$. (We may assume that $k \geq e = \min\{\omega(v_1),\ldots\omega(v_t)\}$ since $\tau_n = gr_n(R)$ for $n < e\}$.

<u>I. The homomorphism θ is injective in degree k.</u>

Applying the induction hypothesis we have $\tau_n = gr_n(R)$ for $n < k$. It implies that $[\tau,\tau]_k = [gr(R),gr(R)]_k$ since both sides of this equality are generated by the brackets of elements of lower degree. Since the kernel of the homomorphism $\tau_k \longrightarrow gr(R)_k/[gr(R),gr(R)]_k$ is exactly $[\tau,\tau]_k$ we see that θ is injective in degree k.

II. The homomorphism θ' is bijective in degree k.

Since $gr(M) = gr(R)/gr([R,R])$, we only have to show that

$$[gr(R),gr(R)]_k = gr_k([R,R]).$$

holds.

In order to do that we will construct a subgroup H of R satisfying the following three conditions:

(H1) H is a free group on $y_1,\dots,y_m$.

(H2) If τ_i is the weight of y_i with respect to the filtration (F_n) of F and if $H_n = H \cap F_n$ then (H_n) is the (Y,τ)–filtration of H.

(H3) If gr(H) is the graded Lie algebra associated to the filtration (H_n) then $gr_n(H) = gr_n(R)$ for $n < k$.

Notice that in view of the Proposition I.4.2, those conditions imply that gr(H) is free Lie algebra on $\eta_1,\dots,\eta_t$ where $\eta_i = inn(y_i)$ with respect to (H_n) $i = 1,2,\dots,m$.

Construction of the group H.

Since τ is a homogeneous ideal of L and by assumption L/τ is Z–free, by Witt's theorem (cf. Lec. cit. Ch.II.3) τ is free Lie algebra with some homogeneous free generating set Y. Since the algebra L is generated by $\xi_1,\dots,\xi_N$, the free Z–module $L_1 \oplus \dots \oplus L_{k-1}$ has finite rank. Hence, the submodule $\tau_1 \oplus \dots \oplus \tau_{k-1}$ has finite Z–basis. It follows that the set $Y \cap \tau_1 \oplus \dots \oplus \tau_{k-1}$ is finite. Denote its elements by $\bar{y}_1,\dots,\bar{y}_m$ $(m \in N)$. If τ_i is the degree of $\bar{y}_i$ for each $i = 1,2,\dots,m$, choose an element $y_i \in T_{\tau_i}$ whose image in $gr_{\tau_i}(R)$ is $\bar{y}_i$. Let H be a subgroup of R generated by $y_1,\dots,y_m$. Let gr(H) be a graded Lie algebra associated to the filtration (H_n) of H where $H_n = H \cap R_n$. Since, by the induction hypothesis, $\tau_n = gr_n(R)$ for $n < k$, and by our construction, $\tau_n = gr_n(R)$ for $n < k$ we get $gr_n(H) = gr_n(R)$ for $n < k$. In order to verify conditions (H1) and (H2) we let E be a free group on $y_1,\dots,y_m$. Let (E_n) be the (y,τ)-filtration of E, and let gr(E) be Lie algebra associated to this filtration. Let z_i be the image of y_i in $gr_{\tau_i}(E)$. Then gr(E) is free Lie algebra with free generating set $z_1,\dots,z_m$ (cf. Loc. cit. Ch.I§.4, Proposition I.4.1.). The canonical surjection $\alpha: E \to H$ mapping y_i to y_i induces surjective homomorphism

$$\overline{\alpha}: gr(E) \to gr(H) \quad (z_i \to \overline{y}_i \quad i = 1,2,\dots,m).$$

Since $gr(H) \subset \tau$ and $\overline{y}_i$ is part of free generating set of τ, we see that $\overline{\alpha}$ is injective. But, this implies that α is injective. Indeed, let e be an element of E such that $\alpha(e) = 1$. Since then, $\overline{\alpha}(inn(e)) = 0$ and $\overline{\alpha}$ is bijective, we see that $e \in E_n$ for all n. Since E is free group, we can represent it as a subgroup of the units of the Magnus algebra A on $\{y_1,\dots,y_m\}$. Thus $\bigcap_{n\geq 1} E_n = 1$, and it implies that $e = 1$.

We want to show that $\alpha(E_1) = H_n$. We have $\alpha(E_1) = H = H_1$. Suppose that $\alpha(E_n) = H_n$ for $n \leq k$. The inclusions $\alpha(E_n) \to H_n$ induce the maps $\alpha(E_n)/\alpha(E_{n+1}) \to H_n/H_{n+1}$ which are injective by the injectivity of $\overline{\alpha}$. Since $\alpha(E_k) = H_k$ we see that $\alpha(E_{k+1}) = H_{k+1}$. Thus, $\alpha(E_n) = H_n$ for all n. This completes verification of (H1), (H2) and (H3).

We return now to the proof of II.

In view of the condition (H3), we have

$$[gr(H), gr(H)]_k = [gr(R), gr(R)]_k.$$

Applying Proposition I.4.2 we get

$$[gr(H),gr(H)]_n = gr_n([H,H]) \text{ for all } n.$$

So, in order to prove II, we only need to show that

$$gr_n([H,H]) = gr_n([R,R])$$

holds for $n \leq k$. Since $H_n = H \cap R_n$, the inclusions $H_n \longrightarrow R_n$ induce the injective homomorphism $f: gr([H,H]) \longrightarrow gr([R,R])$. We want to show that f is surjective in degrees $n \leq k$. The subgroup $[R,R]_n$ is generated modulo $[R,R]_{n+1}$ by the brackets of degree n. Let $v \in R_i$, $w \in R_j$ with $i+j \leq k$ be two elements of R. Since the map $H_n/H_{n+1} \longrightarrow R_n/R_{n+1}$ is bijective for $n < k$, we can find two elements $h \in H_i$, $g \in H_j$ such that $h \equiv v \bmod R_{i+1}$ and $g \equiv w \bmod R_{j+1}$. Using the formulae (I.4.2) and (I.4.3), we see that

$$[h,g] \equiv [v,w] \bmod [R,R] \cap R_{n+1},$$

which implies the surjectivity of f in degrees $n \leq k$ and consequently proves II.

<u>III. The honmomorphism θ is surjective in degree k.</u>

By I and II, to show that θ is surjective in degree k it suffices to show that the composed map $\theta'' = \theta' \cdot \theta$ is surjective in degree k. The conjugate of $r_i \in R$ is the same as the action of $y \in G$ on $\bar{r}_i \in M$, i.e, $xR \cdot r_i[R,R] = xr_ix^{-1}[R,R]$ where $x \in F$, and r_i is a generator of R, $i = 1,2,\ldots,t$. Hence, M as a $Z[G]$–module is generated by $\bar{r}_i = r_i[R,R]$, $i = 1,2,\ldots,t$. Now, if $\overline{m}_k$ is nonzero element of $gr_k(M)$, let m_k be an element of M_k whose image in $gr_k(M)$ is $\overline{m}_k$. We can write

$$(*) \qquad m_k = v_1\bar{r}_1 + \ldots + v_t\bar{r}_t$$

where $v_i \in Z[G]$ $i = 1,2,\ldots,t$. Since $Z[G]_m M_n \subset M_{m+n}$ for all $m,n \in N$, we can choose m_k so that the above expression for m_k involves only those terms $v_i\bar{r}_i$ with $\omega(v_i) + \omega(r_i) \leq k$. Since m_k does not belong to M_{k+1} this expression is not empty. Let q be the smallest integer of the form $\omega(v_i) + \omega(r_i)$, and let S be the set of integers i with $\omega(v_i) + \omega(r_i) = q$. Since the composed map $\psi'' = \psi' \circ \psi$ is surjective, we can chose homogeneous element u_i of $U(L/\tau)$ such that $\psi''(u_i) = \bar{v}_i$ where $\bar{v}_i$ is the image of v_i in $gr_n(Z[G])$ with $n = q - \omega(r_i)$ $i = 1,2,\dots,t$. Put $\xi = \Sigma u_i \bar{\rho}_i$ $(i \in S)$ where $\bar{\rho}_i$ is the image of ρ_i in $\tau/[\tau,\tau]$. Since $\tau/[\tau,\tau]$ is by assumption free $U(L/\tau)$ module on $\bar{\rho}_i (i=1,2,\dots,t)$, we see that $\xi \neq 0$. Since $\deg(\xi) = q$ and the map θ'' is injective in degree q (since $q \leq k$) we see that $0 \neq \theta''(\xi) = \Sigma \psi''(u_i)\theta''(\bar{\rho}_i) = \Sigma \bar{v}_i \theta''(\bar{\rho}_i)(i \in S)$.

Since $\psi''(u_i)\theta''(\bar{\rho}_i)$ is the image of $v_i \cdot \bar{r}_i$ in $gr_q(M)$ and m_k is homogeneous of degree k we get that $q = k$ and $\overline{m}_k = \theta''(\xi)$. Hence θ'' is surjective in degree k.

It follows by induction that θ and θ' are bijective and consequently that $\tau = gr(R)$.

Remark. Since $\tau/[\tau,\tau]$ is free $U(L/\tau)$ module, ψ is compatible with θ and ψ' is compatible with θ', we see that both ψ and ψ' are bijective. Hence, $gr(Z[G]) = U(L/gr(R)) = U(L/\tau)$.

Corollary III.1.

Under the hypothesis of Theorem III.1 the descending central series of G is induced by the J–adic filtration of $Z[G]$ where J (augmentation ideal of $Z[G]$) is the image of $I(F)$ under the canonical map $Z[F] \longrightarrow Z[G]$.

Proof.

Since $gr(G) = gr(F)/gr(R) \doteq gr(F)/\tau$ is a free Z–module, Birkhoff–Witt theorem tells us that the canonical homomorphism $i: gr(G) \longrightarrow U(gr(G)) \cong gr(Z[F])/K$ is injective. We have the canonical homomorphism

β: $gr(G) \to gr\{Z[G])$ defined as follows:

Let $\bar{g}_n$ be the homogeneous element of $gr_n(G)$ and let g_n be an element of G_n whose image in $gr_n(G)$ is $\bar{g}_n$. Define $\beta(\bar{g}_n) = \overline{g_n - 1}$ where $\overline{g_n - 1}$ is the image of $g_n - 1$ in $gr(Z[G])$.

We will show that $\beta = \psi' oi$. If $\bar{g}_n, g_n$ are as above. Let f_n be an element of F_n whose image in G is g_n. Then the image of $\bar{f}_n$ under the canonical injection $gr(F) \longrightarrow gr(Z[F])$ is $\overline{f_n - 1}$ where $\overline{f_n - 1}$ is the image of $f_n - 1$ in $gr(Z[F])$. But $i(\bar{g}_n) = \overline{f_n - 1} \cdot K$ so $\psi' oi(\bar{g}_n) = \overline{g_n - 1}$.

Hence the map β is injective which proves the corollary.

q.e.d.

The theorem just proved suggests the following problem:

Let k be a commutative ring with unity. Let L be a free N–graded Lie algebra over k with free generating set $\{\xi_1, \ldots \xi_N\}$ and let $\rho_1, \ldots \rho_M$ be homogeneous nonzero elements of L. Let $\tau = (\rho_1, \ldots \rho_M)$ be the ideal of L generated by ρ_i, $i = 1,2,\ldots,M$. The question is when the following conditions are satisfied.

(I) L/τ is a free k–module.

(II) $\tau/[\tau,\tau]$ is a free $U(L/\tau)$ module on the images of $\rho_1, \ldots, \rho_M$.

The partial answer to this question was given in Propositions I.3.2 and I.3.3. In order to answer this question we will need a few lemmas.

Lemma III.1.

Let k be a P.I.D. If E is finitely generated k–module and the dimension of $E_{(P)} = E \otimes_k k/(P)$ as a vector space over the field $k/(P)$ is independent of (P), where (P) is a maximal ideal of k, then E is free k–module with rank equal to the dimension of $E_{(P)}$ over $k/(P)$.

Proof.

We will use the Structure Theorem for modules over a PID.

We can write

$$E = TF(E) \oplus T(E)$$

where $T(E)$ is torsion submodule of E and $TF(E)$ is torsion free k–module.

We can write

$$T(E) = k/n_1k \oplus \ldots \oplus k/n_kk$$

where $n_i \in k$, $i=1,2,\ldots k$, $n_1 > 1$ and $n_i | n_{i+1}$ for $i = 1,2,\ldots,k-1$. (The sequence $(n_1,\ldots,n_k)$ is unique up to the units of k). Let P_1 and P_2 be two irreducible elements such that $P_1 | n_1$ and P_2 does not belong to $(n_1,\ldots,n_k)$ – the ideal of k generated by $n_1,\ldots,n_k$. (The element P_2 exists since $(n_1,\ldots,n_k) \neq 1$). Then

$$T(E) \otimes_k k/(P_1) = k/(P_1) \oplus \ldots \oplus k/(P_1) \quad \text{(k–times) and}$$

$$T(E) \otimes_k k/(P_2) = 0.$$

This implies that $T(E) = 0$ and consequently that E is free k–module.

q.e.d.

Let I be the augmentation ideal of $U(L)$ and let $I(\tau)$ be the ideal of $U(L)$ generated by the image of τ under the canonical injection $i:L \longrightarrow U(L)$. The ideal $I(\tau)$ is also the kernel of the canonical surjection $s:U(L) \longrightarrow U(L/\tau)$ (cf. Loc. cit. (I.1.3)).

The injection $\tau \longrightarrow I$ induces the map $\varphi:\tau/[\tau,\tau] \longrightarrow I/I(\tau)\cdot I$ which is $U(L/\tau)$–linear since $\overline{x}\cdot\overline{v} = \overline{[x,v]} = \overline{xv-vx} = \overline{xv}$ for all $x \in L$, $v \in \tau$. The image of φ is $I(\tau)/I(\tau)\cdot I$ which is the kernel of the map $\theta:I/I(\tau)I \longrightarrow U(L)/I(\tau)$ induced by the inclusion $I \longrightarrow U(L)$. The image of θ is $I/I(\tau)$ which is the kernel of the map $\overline{\epsilon}:U(L)/I(\tau) \longrightarrow k$

induced by the augmented map $\epsilon: U(L) \to k$. Hence, we have an exact sequence of $U(L/\tau)$ modules

$$\tau/[\tau,\tau] \xrightarrow{\varphi} I/I(\tau)\cdot I \xrightarrow{\theta} U(L)/I(\tau) \cong U(L/\tau) \xrightarrow{\bar{\epsilon}} k \longrightarrow 0.$$

The ideal I is a direct sum of U(L)–modules $\underset{i}{\oplus} U(L)\xi_i((U(L) \cong \mathrm{Ass}(\xi_1,\ldots,\xi_N))$.

Hence $I(\tau)\cdot I = \underset{i}{\oplus} I(\tau)\xi_i$. Hence if we assume that k is an integral domain then

$$I/I(\tau)I = \underset{i}{\oplus} U(L/\tau)\bar{\xi}_i \quad (\bar{\xi}_i \text{ is the image of } \xi_i \text{ in } I/I(\tau)I).$$

Since by Corollary I.2.5 U(L) is an entire algebra so we get the isomorphism

$$U(L)\xi_i/I(\tau)\xi_i \longrightarrow U(L)/I(\tau)\cdot\bar{\xi}_i = U(L/\tau)\bar{\xi}_i$$

defined by $u\xi_i + I(\tau)\xi_i \longrightarrow (u+I(\tau))\bar{\xi}_i$ for all $u \in U(L)$ and $i = 1,2,\ldots,N$.

Lemma III.2.

Let k be an integral domain and let $M = 1$ i.e., $\tau = (\rho_1)$. If L/τ is a free k–module, then $\tau/[\tau,\tau]$ is free $U(L/\tau)$ module with basis $\bar{\rho}_1$.

Proof.

By Corollary I.2.5 $U(L/\tau)$ is an entire algebra so if $w \in I/I(\tau)\cdot I$, $w \neq 0$ then $U(L/\tau)\cdot w$ is free $U(L/\tau)$ submodule of $I/I(\tau)\cdot I$ with basis w. If we had $\varphi(\bar{\rho}_1) = 0$ then $I(\tau) \subset I(\tau)\cdot I$ which would imply that $I(\tau) \subset I^n$ for all n. Since $\underset{n\leq 1}{\cap} I^n = 0$ we would get $I(\tau) = 0$
which is not true since $\rho_1 \neq 0$. Hence, if $u\bar{\rho}_1 = 0$ then $u\varphi(\bar{\tau}) = 0$ so $u = 0$. It follows that $\tau/[\tau,\tau]$ is free $U(L/\tau)$ module with basis $\bar{\rho}_1$ and that the map φ is injective.

q.e.d.

Lemma III.3.

Let k be a PID and let $\rho_1,\ldots,\rho_M$ be homogeneous elements of L such that conditions (I) and (II) are satsified. If χ_E or $E(t)$ denotes the Euler–Poincaré series of a N–graded free k–module E i.e., $E(t) = \chi_E = \sum_{n=1}^{\infty} \mathrm{rank}(E_n)t^n$, then

1) $1/1-\chi_N = \chi_{U(\tau)}$ where $N = \tau/[\tau,\tau]$, $\tau = (\rho_1,\dots,\rho_M)$.

2) $\chi_{U(L/\tau)} = \chi_{U(L)}/1 + (t^{d_1}+\dots+t^{d_M})\chi_{U(L)}$ where d_i = degree of ρ_i $i = 1,2,\dots,M$.

3) The rank of $(L/\tau)_n$ depends only of the degrees of ξ_i and ρ_i $1 \le i \le N$, $1 \le j \le M$.

<u>Proof.</u>

1) In view of Witt's theorem τ is a free Lie algebra with some homogeneous free generating set $X = \{x_1,x_2,\dots\}$. Since $\tau_n \subset L_n$ for all n and $\mathrm{rank}(L_n)$ is finite we see that $\mathrm{rank}(N_n) \overset{\mathrm{def}}{=} a_n$ and $\mathrm{rank}(U(\tau)_n)$ are finite for all n since $\mathrm{rank}(N_n) = \{x_i \mid d^0(x_i) = n\} = a_n$ and since $U(\tau)$ is free associative algebra on X by Theorem I.3.1, we see that

$$\chi_{U(\tau)} = \sum_{n\geq 0} \sum_{i_1+\dots+i_k=n} a_{i_1}\cdot\ldots\cdot a_{i_k}$$

which is exactly $1/1-\sum_{n\geq 1} a_n t^n$.

2) Since the exact sequence of k–modules $0 \to \tau \to L \to L/\tau \to 0$ splits we can use Corollary I.2.3 to get

$$U(L) = U(\tau)\otimes U(L/\tau)$$

as k–modules. Using the isomorophism $(\bigoplus_{n\geq 0} U(\tau)_n)\otimes(\bigoplus_{n\geq 0} U(L/\tau)_n) \cong \bigoplus_{n,m\geq 0} (U(\tau)_n\otimes U(L/\tau)_m)$ we get

$$\chi_{U(L)} = \chi_{U(\tau)}\cdot\chi_{U(L/\tau)}.$$

Hence, by (1) we can write

$$\chi_{U(L)} = \chi_{U(L/\tau)}/1-\chi_N.$$

The condition (II) implies that we have

$$N = U(L/\tau)\rho_1 \oplus \dots \oplus U(L/\tau)\rho_M.$$

Thus, we get

$$\chi_N = t^{d_1}\chi_{U(L/\tau)} + \dots + t^{d_M}\chi_{U(L/\tau)}.$$

Hence, we get

$$\chi_{U(L)} = \chi_{U(L/\tau)}/1-(t^{d_1}+\dots+t^{d_M})\chi_{U(L/\tau)}.$$

Consequently

$$\chi_{U(L/\tau)} = \chi_{U(L)}/1+(t^{d_1}+\dots+t^{d_M})\chi_{U(L)}$$

which proves (2).

3) We can choose a homogeneous k–basis $\{\gamma_i\}_{i\in I}$ of L/τ and we totally order the index set I. The Birkhoff–Witt theorem implies that the family of elements $\gamma^e = \gamma_1^{e_{i_1}} \cdot \ldots \cdot \gamma_{i_s}^{e_{i_s}}$ with $i_1 > \dots > i_s$ and $e_{i_k} \in N$ is a k–basis of L/τ. Let g_n be the rank of $(L/\tau)_n$, then g_n is equal to the number of families (e_i) such that $n = \Sigma e_i \cdot b_i$, where $b_i = \text{degree}(\gamma_i)$ $(i \in I)$. This is equivalent to the fact that $\chi_{U(L/\tau)}$ may be expressed in the form

$$\chi_{U(L/\tau)} = \prod_{i\in I} \frac{1}{1-t^{b_i}}.$$

because $\prod_{i\in I} \frac{1}{1-t^{b_i}} = \prod_{i\in I} (1+t^{b_i}+\dots)$ and the coefficient of t^n in this product is precisely the number of families (e_i) such that $\Sigma e_i b_i = n$. The number of factors in this product such that $b_i = m$ is the rank g_m of $(L/\tau)_m$ for all $m > 0$ i.e.,

$$\chi_{U(L/\tau)} = \prod_{m=1}^{\infty} \frac{1}{(1-t^m)^{g_m}}.$$

Combining this expression with (2) we get

$$\chi_{U(L)}/1+(t^{d_1}+\dots+t^{d_M})\chi_{U(L)} = \prod_{m=1}^{\infty} \frac{1}{(1-t^m)^{g_m}}.$$

Thus, g_m's depend on the degrees of $\xi_1,\dots,\xi_N$, $\rho_1,\dots,\rho_M$.

q.e.d.

Proposition III.1.

Let k be a PID and let ρ be a homogeneious element of L such that $\rho \notin (P)L$ for any maximal ideal (P) of k. Then if τ is the ideal of L generated by ρ we have:

1) L/τ is a k–free module.

2) $\tau/[\tau,\tau]$ is a free $U(L/\tau)$ module on the image of ρ.

Proof.

The exact sequence $0 \to \tau \to L \to L/\tau \to 0$ tensored with $k/(P)$ gives

$$0 \to \tau(P) \to L(P) \to L/\tau(P) \to 0$$

where

$$\tau(P)=\tau\otimes k/(P)\cong\tau/(P)\tau,\ L(P)=L\otimes k/(P)\cong L/(P)L \text{ and } L/\tau(P)=L/\tau\otimes k/(P).$$

The exact sequence $0 \to [\tau,\tau] \to \tau \to \tau/[\tau,\tau] \to 0$ tensored with $k/(P)$ gives

$$0 \to [\tau(P),\tau(P)] \to \tau(P) \to \tau(P)/[\tau(P),\tau(P)] \to 0$$

for all maximal ideals (P) of k. The algebra L(P) is free Lie algebra over k/(P) on $\xi_1\otimes 1,\dots,\xi_N\otimes 1$.

Since $L(P)/\tau(P)$ is free k/(P) module, and $\bar{\rho} \neq 0$ where $\bar{\rho}$ is the image of ρ in $\tau/(P)\tau$, we can apply Lemma III,2 to get that $\tau(P)/[\tau(P),\tau(P)]$ is free $U(L/\tau(P))$–module with basis $\bar{\rho} + [\tau(P),\tau(P)]$ (for all (P)). Hence, by Lemma III.3 the rank of $(L/\tau(P))_n$ does not depend on a choice of maximal ideal (P) of k.

Hence, by Lemma III.1, L/τ is free k–module.

Now we use Lemma III.2 again to conclude that $\tau/[\tau,\tau]$ is free $U(L/\tau)$–module with basis $\rho + [\tau,\tau]$.

q.e.d.

Now, we return to the example given in Chapter II.

Example III.3. (II.2)

Let L be Lie algebra over the integers with the presentation $<x_1,x_2,x_3;\ 2x_1 = [x_2,x_3]>$. Let 2,1 and 1 be the degrees of x_1,x_2 and x_3 respectively. We want to show that L is Z–free module. By Proposition III.1 it suffices to show that $2x_1 - [x_2,x_3] \notin (p)L(X)$ for any prime number p where $L(X)$ is a free Lie algebra on $X = \{x_1,x_2,x_3\}$. We choose a total order on X such that $x_2 < x_3$. Using this total order of X we construct a basic family R in $\Gamma(X)$ where $\Gamma(X)$ is a free magma on X.

Hence, x_1 and $[x_2,x_3]$ are elements of R.

If $2x_1 - [x_2,x_3] \in (p)L(x)$ for some prime number p then we could write

$$2x_1 - [x_2,x_3] = pn_1\gamma_{i_1} + \ldots + p\cdot n_k\cdot\gamma_{i_k}$$

where $n_i \in Z$, $\gamma_{i_j} \in R$, $j = 1,2,\ldots,k$. This would imply that $(2-p\cdot n_m) = 0$ and $(1+p\cdot n_q) = 0$ for some $1 \leq m,q \leq k$, $m \neq q$. But the second equality is impossible.

q.e.d.

Now, let k be a commutative ring and let L be a free N–graded Lie algebra on $\{\xi_1,\ldots,\xi_N\}$ over k. Let $\rho_1,\ldots,\rho_M$ be nonzero homogeneous elements of L and let τ be the ideal of L generated by $\rho_1,\ldots\rho_M$.

Definition III.1.

We call the elements $\rho_1,\dots,\rho_M$ <u>strongly free</u> if and only if:

(I) L/τ is a free k–module.

(II) $\tau/[\tau,\tau]$ is a free $U(L/\tau)$–module on the images of $\rho_1,\dots,\rho_M$.

Let $A(t)$, $B(t)$ and $C(t)$ denote formal power series in $Z[[t]]$.

<u>Definition III.2.</u>

1) We write $A(t) \geq_T B(t)$ if and only if $a_n - b_n \geq 0$ for all n were $A(t) = \sum_{n=0}^{\infty} a_n t^n$ and $B(t) = \sum_{n=0}^{\infty} b_n t^n$.

2) We write $A(t) \geq B(t)$ if and only if:

either $a_n - b_n \geq 0$ for all n, or $a_{n_0} > b_{n_0}$ and $a_n = b_n$ for $n < n_0$ (some n_0).

<u>Lemma III.4.</u>

1) If $A(t) \geq_T B(t)$ and $C(t) \geq_T 0$ then $A(t)\cdot C(t) \geq_T B(t)\cdot C(t)$ with equality only if $A(t) = B(t)$ or $C(t) = 0$.

2) If $A(t) \geq B(t)$ and $C(t) \geq 0$ then $A(t)\cdot C(t) \geq B(t)\cdot C(t)$ with equality only if $A(t) = B(t)$ or $C(t) = 0$.

3) If $A(t)$ and $B(t)$ are invertible in $Z[[t]]$ and $B(t) > 0$ then $A(t) \geq B(t)$ if and only if $A(t)^{-1} \leq B(t)^{-1}$ and equality occurs only if $A(t) = B(t)$.

4) If $A(t) \geq_T B(t)$ then $A(t)+C(t) \geq_T B(t)+C(t)$.

If $A(t) \geq B(t)$ then $A(t)+C(t) \geq B(t)+C(t)$.

If $C > 0$ then $A(t) \geq_{(T)} B(t)$ implies $C\cdot A(t) \geq_{(T)} C\cdot B(t)$.

<u>Proof.</u>

1) For all natural numbers m we have

$$a_0C_m+\dots+a_mC_0-(b_0C_m+\dots+b_mC_0) = C_0(a_m-b_m)+\dots+C_m(a_0-b_0) \geq 0.$$

2) Let n_0 be the smallest natural number such that $a_{n_0} > b_{n_0}$ and let m_0 be the smallest natural number such that $C_{m_0} > 0$. Then

$C_{m_0} a_{n_0} > C_{m_0} b_{n_0}$ and hence

$C_0 a_{n_0+m_0} + C_1 a_{n_0+m_0-1} + \ldots + C_{m_0+n_0} a_0 >$

$C_0 b_{n_0+m_0} + C_1 b_{n_0+m_0-1} + \ldots + C_{n_0+m_0} b_0$

which proves (2).

3) If $A(t) \geq B(t)$ then $A(t)^{-1} > 0$ so by (2): $1 \geq A(t)^{-1} B(t)$. Applying (2) again we get

(*) $$B(t)^{-1} \geq A(t)^{-1}.$$

In the same way we prove that (*) implies $A(t) \geq B(t)$.

4) Trivial.

q.e.d.

Lemma III.5.

Let k be a field. Then

$$\chi_{U(L/\tau)} \geq \chi_{U(L)}/1 + (t^{d_1} + \ldots + t^{d_M})\chi_{U(L)}$$

with equality if and only if the elements $\rho_1, \ldots \rho_M$ are strongly free.

Proof.

Condition (I) is obviously true since k is a field. Proceeding as in the proof of Lemma III.3 we get

$$\chi_{U(L)} = \chi_{U(L/\tau)}/1 - \chi_N$$

where $N = \tau/[\tau,\tau]$. Since N as a $U(L/\tau)$–module is generated by the images of $\rho_1, \ldots, \rho_M$, we get the k–linear graded surjective map

$$\varphi:(U(L/\tau))^1 \oplus \ldots \oplus (U(L/\tau))^M \to N$$

where $(U(L/\tau))^i \cong U(L/\tau)$ $i = 1,2,\ldots,M$; defined by $(u_1,\ldots,u_M) \to u_1\bar{\rho}_1+\ldots+u_M\bar{\rho}_M$ (where $u_i \in U(L/\tau)$). If we want to make the map φ graded of degree zero we only need to define new gradings on $(U(L/\tau))^i$ by $(U(L/\tau))^i_n = U(L/\tau)_{n-d_i}$ where d_i is the degree of ρ_i, $i = 1,2,\ldots,M$.

By surjectivity of φ we get

$$\chi_{U(L/\tau)^1}+\ldots+\chi_{U(L/\tau)^M} \geq_T \chi_N$$

with equality if and only if φ is an isomorphism. Hence,

$$(t^{d_1}+\ldots+t^{d_M})\chi_{U(L/\tau)} \geq_T \chi_N.$$

It follows that

$$1-\chi_N \geq_T 1-(t^{d_1}+\ldots+t^{d_M})\cdot\chi_{U(L/\tau)}$$

and hence

$$\chi_{U(L)}\cdot(1-\chi_N) \geq_T \chi_{U(L)} - (t^{d_1}+\ldots+t^{d_M})\chi_{U(L)}\cdot\chi_{U(L/\tau)}$$

Since $\chi_{U(L)}(1-\chi_N) = \chi_{U(L/\tau)}$ (cf. Loc. cit. the proof of Lemma III.3) we see that

$$\chi_{U(L/\tau)}(1+(t^{d_1}+\ldots+t^{d_M})\chi_{U(L)}) \geq_T \chi_{U(L)}.$$

Applying Lemma III.4 we get

$$\chi_{U(L/\tau)} \geq \chi_{U(L)}/1+(t^{d_1}+\ldots+t^{d_M})\chi_{U(L)}$$

with equality only if φ is an isomorphism, i.e., if and only if $\rho_1,\ldots,\rho_M$ are <u>strongly free</u>.

q.e.d.

<u>Proposition III.2.</u>

Let k be a principal ideal domain. Let L be the free, N–graded Lie algebra on $\{\xi_1,\ldots\xi_N\}$. Let $\rho_1,\ldots,\rho_M$ be nonzero homogeneous elements of L of degrees

$d_1, \dots d_M$ respectively.

If for all maximal ideals (P) of k we have

$$\chi_{U(L/\tau)(P)} = \chi_{U(L)}/1 + (t^{d_1} + \dots + t^{d_M})\chi_{U(L)}$$

then the elements $\rho_1, \dots, \rho_M$ are strongly free.

Proof.

The ideal $\tau(P) = \tau \otimes_k k/(P)$ is free Lie subalgebra of L(P). Since the rank of L_n is equal to the rank of $L_n \otimes k/(P)$ we apply Lemma III.5 to conclude that the elements $\bar{\rho}_1, \dots, \bar{\rho}_M$ are strongly free where $\bar{\rho}_i$ is the image of ρ_i in $\tau/(P)\tau$ for i = 1,2,...,M. Hence, by Lemma III.3, the rank of $(L/\tau(P))_n$ does not depend on a choice of the maximal ideal (P) of k. Applying Lemma III.1 we conclude that L/τ is a free k–module.

The elements $\rho_i + [\rho,\rho]$ generate $\tau/[\tau,\tau]$ as a $U(L/\tau)$ module, i = 1,2,...,M. Hence, in order to show that condition (II) hold, we only need to prove that they are $U(L/\tau)$–linearly independent. The relation

$$u_1(\rho_1 + [\tau,\tau]) + \dots + u_M(\rho_M + [\tau,\tau]) = 0 \quad u_i \in U(L/\rho) \quad i = 1,2,\dots,M$$

tensored with k/(P) would imply that

$$u_1 \otimes 1(\rho_1 \otimes 1 + [\tau(P),\tau(P)]) + \dots + u_M \otimes 1(\rho_M \otimes 1 + [\tau(P),\tau(P)]) = 0.$$

But, the elements $\rho_i \otimes 1 + [\tau(P),\tau(P)]$, i = 1,2,...,M, are $U(L/\tau)(P)$–linearly independent so $u_i \otimes 1 = 0$, i = 1,2,...,M. Since L/τ is k–free module, the algebra $U(L/\tau)$ is k–free by Birkhoff–Witt Theorem. Thus, $u_i \otimes 1 = 0$ implies $u_i = 0$.

q.e.d.

In view of this proposition and Lemma HI.5 we consider the following problem: Let $Ass(\xi_1, \dots, \xi_N) = V$ be free associative algebra over a field k. The algebra V is given some N–grading by associating positive degrees to the elements

$\xi_1,\dots,\xi_N$. Let $\alpha_1,\dots,\alpha_M$ be nonzero homogeneous elements of V of degrees $d_1,\dots,d_M$ respectively with $d_i \geq 1$, $i = 1,2,\dots,M$. Let R be two–sided ideal of V generated by $\{\alpha_1,\dots,\alpha_M\}$. We call the elements strongly free if and only if

$$V/R(t) = V(t)/1 + (t^{d_1}+\dots+t^{d_M})V(t).$$

where $V(t)$ and $V/R(t)$ are Euler–Poincaré series of V and V/R respectively.

We want to know when the elements $\alpha_1,\dots,\alpha_M$ are strongly free.

We will need some preliminaries on locally finite, connected, N–graded k–algebras. The main references for this paragraph are [1] and [2].

Definition III.4.

Let k be a field and let $A = \bigoplus_{n\geq 0} A_n$ be N–graded associative algebra over k. Then

1) A is called connected if $A_0 = k$.

2) A is called locally finite if dimension of A_n is finite for all n.

As in [2] we will denote the category of all locally finite, connected k–algebras by C.G.A.

Let A, B be in C.G.A. We can write $A = k\oplus\overline{A}$ and $B = k\oplus\overline{B}$ where $\overline{A} = \bigoplus_{n\geq 1} A_n$, $\overline{B} = \bigoplus_{n\geq 1} B_n$. By the coproduct $A\sqcup B$ in C.G.A. of A and B we will mean $A\sqcup B = k\oplus\overline{A}\oplus\overline{B}\oplus(\overline{A}\otimes\overline{B})\oplus(\overline{B}\otimes\overline{A})\oplus(\overline{A}\otimes\overline{B}\otimes\overline{A})\oplus\dots$ where all tensors are taken over k.

Lemma III.6.

If $A, B \in$ C.G.A. then

(*) $$[(A\sqcup B)(t)]^{-1} = [A(t)]^{-1} + [B(t)]^{-1} - 1.$$

Proof.

The formula (*) is equivalent to

(**) $$A(t)\cdot B(t)(1+A\sqcup B(t)) = A\sqcup B(t)(A(t)+B(t)).$$

In order to prove (**) it suffices to prove that there is an isomorphism

(***) $$A\otimes(k\oplus A\sqcup B)\otimes B \cong A\sqcup B\otimes(A\oplus B) = (A\sqcup B\otimes A)\oplus(A\sqcup B\otimes B)$$

of vector spaces over k. If we write $A\sqcup B = k\oplus\overline{A\sqcup B}$ then left hand side of (***) becomes

$$(k\oplus\overline{A})\otimes(k\otimes k\oplus\overline{A\sqcup B})\otimes(k\oplus\overline{B})$$

$$= k\otimes k\oplus\overline{A\sqcup B}\oplus\overline{B}\oplus\overline{B}\oplus(\overline{A\sqcup B}\otimes\overline{B})\oplus\overline{A}\oplus\overline{A}\oplus(\overline{A}\otimes\overline{A\sqcup B})\oplus(\overline{A}\otimes\overline{B})\oplus(\overline{A}\otimes\overline{B})\oplus(\overline{A}\otimes\overline{A\sqcup B}\otimes\overline{B}).$$

The right–hand side of (***) becomes

$$(k\oplus\overline{A\sqcup B})\otimes(k\otimes k\oplus\overline{A}\oplus\overline{B})$$

$$= k\otimes k\oplus\overline{A}\oplus\overline{B}\oplus\overline{A\sqcup B}\oplus\overline{A\sqcup B}\oplus(\overline{A\sqcup B}\otimes\overline{A})\oplus(\overline{A\sqcup B}\otimes\overline{B}).$$

Since

$$\overline{A}\oplus\overline{B}\oplus(\overline{A}\otimes\overline{B})\oplus(\overline{A}\otimes\overline{B})\oplus(\overline{A}\otimes\overline{A\sqcup B}\otimes\overline{B}) \cong \overline{A\sqcup B}$$

as vector spaces over k we proved (***)

q.e.d.

Let now $A = \mathrm{Ass}(\alpha_1,\dots\alpha_M)$ be a free associative algebra on $\alpha_1,\dots,\alpha_M$ and let d_i be the degree of α_i, $i = 1,2,\dots,M$. We can write

$$A(t) = 1 + t^{d_1}+\dots+t^{d_M} + (t^{d_1}+\dots+t^{d_M})^2+\dots$$

and hence

$$A(t) = 1/1-(t^{d_1}+\dots+t^{d_M}).$$

If B is any associative algebra over k generated by $\beta_1,\dots,\beta_M$ with $d^0(\beta_i) = d_i$, $i = 1,2,\dots,M$ then

$$B(t) \leq 1/1-(t^{d_1}+\ldots+t^{d_M})$$

with equality if and only if B is isomorphic to A via the canonical map defined by $\alpha_i \longrightarrow \beta_i$, $i = 1,2,\ldots M$.

Let us introduce the following notation:

1) $V = Ass(\xi_1,\ldots\xi_N)$.

2) $Ass(\alpha) = Ass(\alpha_1,..\alpha_M)$ – free associative k–algebra on $\{\alpha_1,\ldots,\alpha_M\}$.

3) $R = V\alpha V$ is the two–sided ideal of V generated by $\{\alpha_1,\ldots,\alpha_M\}$.

4) $U = V/V\alpha V$.

We have the canonical map $\varphi{:}Ass(\alpha) \longrightarrow V$ sending α_i to α_i for $i = 1,2,\ldots,M$. We hve the canonical projection $\pi{:}V \longrightarrow U$ which is graded of degree zero. Let s be any section $s{:}U \longrightarrow V$ of degree zero (such a map exists since we are working over a field).

Let $f = \varphi \sqcup s$ be the canonical map from $Ass(\alpha)\sqcup U$ into V. We see that $f(\gamma_1 u_1 \gamma_2 u_2\ldots) = \varphi(\gamma_1)s(u_1)\varphi(\gamma_2)s(u_2)\ldots$, where $u_i \in U$ and $\gamma_i \in Ass(\alpha)$ ($i \in J$–some finite set).

Lemma III.7.

The map $f = \varphi \sqcup s$ is surjective.

Proof.

We will proceed by induction on degrees.

The map f is obviously surjective in degree 1.

Suppose that f is surjective in degrees $k \leq n$, and let $v \in V_{n+1}$. Let $h = s\pi(v)$.

Since $\pi(v-h) = \pi(v)-\pi(h) = \pi(v) - \pi \cdot s \cdot \pi(v) = 0$ we see that $v - h \in V\alpha V$.

Hence, we can write

$$v - h = \Sigma u_i \alpha_{j_i} w_i \quad (i \in I\text{—finite set})$$

where $u_i, w_i \in V$ are homogeneous ($i \in I$). Since $d_i \geq 1$ for $i = 1,2,\dots,M$, we see that $d^0(u_i)$, $d^0(w_i) \leq n$ ($i \in I$). Applying the induction hypothesis we can find elements u_i', $w_i' \in \mathrm{Ass}(\alpha) \sqcup U$ such that $f(u_i') = u_i$ and $f(w_i') = w_i$ ($i \in I$). It follows that

$$v - h = f(\Sigma u_i' \alpha_{j_i} w_i') \quad (i \in I)$$

which proves our lemma.

q.e.d.

Above, we defined the map f using any section associated to the projection π. There is no canonical choice of s but the next lemma will show that the particular choice of s is not very important, at least for our purposes.

Lemma III.8.

The following are equivalent:

1) $\mathrm{Ass}(\alpha) \sqcup U \cong V$ as graded vector spaces.

2) f is injective for some choice of s.

3) f is injective for any choice of s.

Proof.

That (3) implies (2) and (2) implies (1) is obvious. To see that (1) implies (3) notice that f is a surjection between vector spaces of equal rank in every homogeneous component, hence an isomorphism.

q.e.d.

Lemma III.9.

1) $(\mathrm{Ass}(\alpha) \sqcup U)(t) \geq V(t)$ with equality if and only if the elements $\alpha_1, \dots, \alpha_M$

are strongly free.

2) As a coproduct of the proof of (1) we hve

$$V(t)/1+(t^{d_1}+\ldots+t^{d_M})V(t)\le U(t)$$

with equality if and only if $\alpha_1,\ldots,\alpha_M$ are strongly free.

Proof.

Since f is a surjective map of degree zero we have

$$(\mathrm{Ass}(\alpha)\sqcup U)(t)\ge_T V(t)$$

with equality if and only if f is an isomorphism.

Hence, by Lemma III.4 we have

$$[(\mathrm{Ass}(\alpha)\sqcup U)(t)]^{-1}\le[V(t)]^{-1}.$$

By Lemma III.6 we get

$$[\mathrm{Ass}(\alpha)(t)]^{-1}+[U(t)]^{-1}-1\le[V(t)]^{-1}$$

and hence

$$1-(t^{d_1}+\ldots+t^{d_M})+[U(t)]^{-1}-1\le[V(t)]^{-1}.$$

It follows that

$$V(t)\le U(t)(1+(t^{d_1}+\ldots+t^{d_M})V(t))$$

and consequently

$$V(t)/1+(t^{d_1}+\ldots+t^{d_M})V(t)\le U(t)$$

with equality if and only if $\alpha_1,\ldots,\alpha_M$ are strongly free.

q.e.d.

Definition III.5.

If $\alpha_1,\ldots,\alpha_M$ are monomials in $\xi_1,\ldots,\xi_N$, of degrees greater than or equal to 1, then $\alpha_1,\ldots,\alpha_M$ are said to be combinatorially free if and only if

1) no α_i is a submonomial of α_j for $i \neq j$, and

2) whenever $\alpha_i = x_1y_1$ and $\alpha_j = x_2y_2$ where x_1,y_1,x_2,y_2 are monomials of degree ≥ 1, we have $x_1 \neq y_2$.

<u>Proposition III.2.</u>

If $\alpha_1,\ldots,\alpha_M$ are nonempty monomials in $\xi_1,\ldots,\xi_N$, then $\alpha_1,\ldots,\alpha_M$ are combinatorially free if and only if $\alpha_1,\ldots,\alpha_M$ are strongly free.

<u>Proof.</u>

Let $\pi: V \longrightarrow V/V\alpha V$ be the projection map. A k–basis for $U = V/V\alpha V$ is the π–image of the set $M = \{$all monomials in $\xi_1,\ldots,\xi_N$, which do not have any α_i as a submonomial$\}$. Let $s: U \longrightarrow V$ be the section defined by $s(\pi(x)) = x$ for all $x \in M$. If G is the subalgebra of V generated by $\alpha = \{\alpha_1,\ldots,\alpha_M\}$ we then have the canonical surjection

$$\varphi: \mathrm{Ass}(\alpha) \longrightarrow G \quad (\alpha_i \longrightarrow \alpha_i,\ i = 1,2,\ldots,M).$$

The map $f = \varphi \sqcup s: \mathrm{Ass}(\alpha) \sqcup U \longrightarrow V$ is surjective by Lemma III.7, and it is injective if and only if $\alpha_1,\ldots,\alpha_M$ are strongly free (Lemma III.9).

A k–basis for $\mathrm{Ass}(\alpha) \sqcup U$ consists of all sequences $(\gamma,g) = \gamma_0 \cdot g_1 \cdot \gamma_1 \cdot \ldots \cdot \gamma_{m-1} \cdot g_m$ such that: $m \geq 1$, $\gamma_0 \in M(\alpha)$, $\gamma_i \in M(\alpha) - \{1\}$ for $i > 0$, $s(g_m) \in M$ and $s(g_j) \in M - \{1\}$ for $j < M$ where $M(\alpha)$ is a free monoid on $\alpha = \{\alpha_1,\ldots,\alpha_M\}$. Let $M(\xi)$ be a free monoid on the set $\xi = \{\xi_1,\ldots,\xi_N\}$.

To show that f is an isomorphism is equivalent to showing that the representation of any element $x \in M(\xi)$ as a product

$$(*) \qquad \varphi(\gamma_0) \cdot s(g_1) \cdot \ldots \cdot \varphi(\gamma_{m-1}) \cdot s(g_m)$$

is unique.

Suppose that $\alpha_1,\ldots,\alpha_M$ are combinatorially free. To see that the representation of any $x \in M(\xi)$ as a product of the form (*) is unique, suppose the contrary. Choose $x \in M(\xi)$ so that the length of x is minimal among the elements of $M(\xi)$ with multiple representations, and let

$$x = \varphi(\gamma_0)\cdot s(g_1)\cdot\ldots\cdot\varphi(\gamma_{m-1})\cdot s(g_m) = \varphi(\gamma_0')\cdot s(g_1')\cdot\ldots\cdot\varphi(\gamma_{n-1}')\cdot s(g_n')$$

be two distinct representations of x. We may assume that the length $l(x)$ of x is greater than zero since clearly $1 = 1\cdot 1$ is unique.

Case 1. $\gamma_0 = \gamma_0' = 1.$

In this case, we must have $m,n > 0$, hence one of $s(g_1)$ and $s(g_1')$, say $s(g_1)$ is a submonomial of the other. Hence, we can write $s(g_1') = s(g_1)\cdot s(h_1)$ where $s(h_1) \in M$. Thus, the element

$$y = \varphi(\gamma_1)\cdot s(g_2)\cdot\ldots\cdot\varphi(\gamma_{m-1})\cdot s(g_m) = s(h_1)\cdot\varphi(\gamma_1')\cdot\ldots\cdot\varphi(\gamma_{n-1}')\cdot s(g_n')$$

also has two distinct representations, contradicting the minimality of x.

Case 2. $\gamma_0 \neq 1$ and $\gamma_0' \neq 1.$

In this case, we can write $\gamma_0 = \alpha_{i_1}\cdot\ldots\cdot\alpha_{i_s}$ and $\gamma_0' = \alpha_{j_1}\cdot\ldots\cdot\alpha_{j_t}$.

If $\alpha_{i_1} = \alpha_{j_1}$ then x is not minimal. If $\alpha_{i_1} \neq \alpha_{j_1}$, then one of them is a submonomial of the other contradicting the fact that $\alpha_1,\ldots,\alpha_M$ are combinatorially free.

Case 3. $\gamma_0 \neq 1,\ \gamma_0' = 1.$

Le us write $\gamma_0 = \alpha_{i_1}\cdot\ldots\cdot\alpha_{i_s}$ and $\gamma_1' = \alpha_{j_1}\cdot\ldots\cdot\alpha_{j_t}$. We cannot have $l(s(g_1')) \geq l(\alpha_{i_1})$ for if we did, then α_{i_1} would be submonomial of $s(g_1')$ contradicting the fact that $s(g_1') \in M$. Hence, $\alpha_{i_1} = s(g_1')\cdot x_1$ for some $x_1 \in M(\xi) - \{1\}$.

If $l(\alpha_{i_1}) \geq l(s(g_1')\cdot\alpha_{j_1})$, then α_{j_1} is a submonomial of α_{i_1} contradicting the fact that $\alpha_1,\ldots,\alpha_M$ are combinatorially free. Hence, $s(g_1')\cdot\alpha_{j_1} = \alpha_{i_1}\cdot x_2$ for some $x_2 \in M(\xi)-\{1\}$. It follows that $\alpha_{j_1} = x_1x_2$ and $\alpha_{i_1} = s(g_1')\cdot x_1$. But this contradicts the fact that $\alpha_1,\ldots,\alpha_M$ are combinatorially free.

Case 4. $\gamma_0 = 1, \gamma_0' \neq 1$.

As above.

Conversely, suppose that $\alpha_1,\ldots,\alpha_M$ are not combinatorially free.

If α_i is a submonomial of α_j, then $\alpha_j = x\cdot\alpha_i\cdot y$ for some $x,y \in M(\xi)$ and we see that α_j' has two representations as a product of the form (*).

If $\alpha_i = x\cdot y$ and $\alpha_j = z\cdot x$ for some $x,y,z \in M(\xi)$ with $y,z, \in M(\xi)-\{1\}$, then $zxy = \alpha_j\cdot y = z\cdot\alpha_i$ has two distinct representations of the form (*).

q.e.d.

Lemma III.10.

Let $f{:}V \to H$ be a surjective homomorphism of elements of C.G.A. where V is a free associative algebra on a totally ordered set S. Let $M(S)$ be the free monoid on S ordered lexicographically. Then:

1) There exists a hereditary subset M of $M(S)$ such that $f(M)$ is a k–basis of H.

2) If $x \in M(S) - M$, then $f(x) \in k\langle f(y){:}y \in M$ and $y < x\rangle$, where $k\langle S_1\rangle$ denotes the vector subspace of H generated by the set S_1.

Proof.

We define M inductively. Let $x_1 = 1$ and suppose that $x_1,\ldots,x_n$ have already been chosen. Let x_{n+1} be the smallest element of $M(S)$ such that $f(x_{n+1}) \notin k\langle f(x_1),\ldots,f(x_n)\rangle$. Clearly, conditions (1) and (2) are satisfied. To see that M is hereditary, suppose the contrary. Choose $x \in M$ such that

$x = v \cdot y \cdot w$ where $v,y,w \in M(S)$ and $y \notin M$. We can write $f(y) = \sum_{u_i<y} k_i f(u_i)$ for some $u_i \in M$, $k_i \in k$.

Hence

$$f(x) = \sum_{u_i<y} k_i \cdot f(v \cdot u_i \cdot w).$$

Since $u_i < y$ implies $v \cdot u_i \cdot w < v \cdot y \cdot w = x$, we see that $f(x)$ is a linear combination of f–images of smaller monomials. This contradicts our choice of M. q.e.d.

Let $\alpha_1 \ldots, \alpha_M$ be homogeneous elements of the free algebra $\mathrm{Ass}(\xi_1,\ldots \xi_N)$ over a field k. Let us totally order the set $\xi = \{\xi_1,\ldots,\xi_N\}$ and then order the free monoid $M(\xi)$ lexicographically. Let $\hat{\alpha}_1$ denote the highest term of α_i, $i = 1,2,\ldots,M$.

Proposition III.3.

If $\hat{\alpha}_1,\ldots,\hat{\alpha}_M$ are combinatorially free then $\alpha_1,\ldots\alpha_M$ are strongly free.

Proof.

Let M be the hereditary subset of $M(\xi)$ as constructed in Lemma III.10. Let $\hat{M} = \{x \in M(\xi)$: no $\hat{\alpha}_i$ is a submonomial of $x\}$. Then the images of the elements of $\hat{M}$ under the canonical projection $\hat{\pi}: V \longrightarrow V/V\hat{\alpha}V = \hat{U}$ form a k–basis for $\hat{U}$ where $\hat{\alpha} = \{\hat{\alpha}_1,\ldots,\hat{\alpha}_M\}$. The image of M under the canonical projection $\pi: V \longrightarrow V/V\alpha V = U$ form a k–basis for U. Since

$$0 = \pi(\alpha_i) = k_i \cdot \pi(\hat{\alpha}_i) + \pi \text{(a linear combination of smaller monomials)}$$

for some nonzero $k_i \in k$, we see that $\pi(\hat{\alpha}_i) \in k<\{P(x): x \in M \text{ and } x<\hat{\alpha}_i\}>$. Thus, $\hat{\alpha}_i \notin M$ for $i = 1,2,\ldots,M$. It follows that $M \subset \hat{M}$ and consequently that rank $(U_n) \leq \mathrm{rank}\,(\hat{U}_n)$ for all n. Let d_i be the degree of α_i, $i = 1,2,\ldots,M$. By Proposition III.2 the elements $\hat{\alpha}_1,\ldots,\hat{\alpha}_M$ are strongly free. Hence

$$\hat{U}(t) \leq_T \hat{U}(t) = V(t)/1 + (t^{d_1}+\dots+t^{d_M})V(t).$$

By Lemma III.9 this can only happen if $U(t) = V(t)/1 + (t^{d_1}+\dots+t^{d_M})V(t)$, i.e, if $\alpha_1,\dots,\alpha_M$ are strongly free.

q.e.d.

Example III.4.

Let L be the free Lie algebra on $\xi_1,\dots,\xi_N$ over a field k, and let $\alpha_1,\dots,\alpha_{N-1}$ be elements of the following form:

(*) $$\alpha_i = \sum_{j=1}^{N} a_{i_j} \cdot [\xi_i,\xi_j]$$

where $a_{i_j} \in k$, $i = 1,2,\dots,N-1$; $j = 1,2,\dots,N$ and $a_{i_j} = a_{j_i}$.

Let G be a graph with vertices $\{1,2,\dots,N\}$ and let us join the vertices i and j if $i \neq j$ and $a_{i_j} \neq 0$. We say that G is connected if and only if for each pair of edges, there exists a way between them.

We will show that:

if G is connected then $\alpha_1,\dots,\alpha_{N-1}$ are strongly free.

We choose a maximal subtree T of G and we relabel the vertices so that for every m the vertex v_m is T–connected to one of $v_{m+1},\dots,v_N$ (i.e., the direct way in T between v_m and one of $v_{m+1},\dots,v_N$ exists). Next, we label each vertex "high" or "low" inductively as follows: v_N is "high". If v_j is labeled "high" or "low" for $j > m$, then we label v_m "high" if it is not G–connected to any "high" vertex v_j with $j > m$ (i.e., there is no direct way in G between v_m and any "high" labeled vertex v_j with $j > m$ or in other words $a_{m_j} = 0$ if $j > m$ and v_j is "high"). Otherwise, we label v_m "low". It follows that no two high vertices are G–connected.

Next we label ξ_i "high" or "low" depending on whether v_i is "high" or "low". We order the set $\{\xi_1,\dots,\xi_N\}$ as follows: $\xi_i < \xi_j$ if ξ_i is low and ξ_j is high, and we endow low and high elements with the natural index order (for example $\xi_3 < \xi_5$). Suppose that v_m is "high" with $m < N$. Then $\alpha_m = \Sigma a_{m_j}[\xi_m,\xi_j]$ with ξ_m "high" and ξ_j "low" and $a_{m_j} \neq 0$ for some $j > m$.

Hence $\hat{\alpha}_m = \xi_m\xi_j$ with ξ_j "low", ξ_m "high" and $j > m$.

Suppose that v_m is "low". Then $\hat{\alpha}_m = \xi_j \cdot \xi_m$ with ξ_j "high", ξ_m "low" and $j > m$.

We claim that $\hat{\alpha}_1,\dots,\hat{\alpha}_{N-1}$ are combinatorially free.

Indeed, if $\hat{\alpha}_i = \hat{\alpha}_j$ for some $1 \le i, j \le N-1$ with $i < j$, then we cannot have both ξ_i and ξ_j high or low: if $\hat{\alpha}_i$ is "high" then $\hat{\alpha}_i = \xi_i \cdot \xi_j$ and if $\hat{\alpha}_i = \hat{\alpha}_j$ then $\hat{\alpha}_j = \xi_i \xi_j$ contradicting that $i < j$. If $\hat{\alpha}_i$ is "low" then $\hat{\alpha}_i = \xi_j \cdot \xi_i$ and if $\hat{\alpha}_i = \hat{\alpha}_j$ then $\hat{\alpha}_j = \xi_j \cdot \xi_i$ contradicting that $i < j$.

It follows that $\hat{\alpha}_1,\dots,\hat{\alpha}_{N-1}$ are all distinct, and since they are all of degree two we see that none of them is a submonomial of the other.

If $\hat{\alpha}_i = \xi_m \cdot \xi_n$ then ξ_m is always "high" and ξ_n is always "low". Hence, the second part of Definition III.5 is also satisfied.

By Proposition III.3 the elements $\alpha_1,\dots,\alpha_{N-1}$ are strongly free.

Let L be the free Lie algebra on $\{\xi_1,\dots,\xi_N\}$ over the integers, and let $\alpha_1,\dots,\alpha_{N-1}$ be elements of the form (*) with $a_{i_j} \in Z$. Let <u>G(p)</u> denote the reduced graph whose edges are $\{1,2.,,,.N\}$ and whose vertices i and j are joined if and only if $a_{i_j} \equiv 0 \bmod(p)$.

<u>If G(p) is connected for all prime numbers p then by Proposition III.2 the</u>

elements $\alpha_1,\ldots,\alpha_{N-1}$ are strongy free.

We will establish now a necessary and sufficient condition for $G(p)$ to be connected for all primes p.

Let B be the matrix with N rows labeled by the natural numbers $1,2,\ldots,N$, and $\binom{N}{2}$ columns labeled by pairs of natural numbers (i,j) such that $i < j$ and $1 \leq i,\ j \leq N$. The position $(i,(i,j))$ and $(j,(i,j))$ are equal to a_{i_j} and $-a_{i_j}$ respectively $(i < j)$. Otherwise they are equal to zero. Since the sum of the rows is zero, the rank of B is at most $N-1$. The relation "the vertex v_m is connected (not necessarily directly) with v_j" is an equivalence relation. Suppose that $G(p)$ is disconnected for some p. Let $B(p)$ be the matrix B reduced modulo p. Then, there exist at least two equivalence classes in the set of vertices: one can be represented as

a $k\times\binom{k}{2}$ submatrix B_k of $B(p)$ and the second can be represented as a $l\times\binom{l}{2}$ submatrix B_l of $B(p)$ with $k+l \leq N$. The submatrices B_k and B_l are disjoint. Since the sums of the rows in B_k and B_l are both zero, we see that $rk(B_k) + rk(B_l) \leq k-1+l-1 \leq N-2$. Hence, if we prove that $rk(B_k) = k-1$, we will prove the following statement: G(p) is connected for every prime number p if and only if $rk(B(p)) = N-1$ where $B(p)$ is the matrix B reduced modulo p.

We relabel the rows $1,2,\ldots,N$ such that $1,2,\ldots,k$ are the rows of $B_k (k \leq N)$.

Suppose that we have the relation

$$(**) \qquad b_1R_{i_1}+\ldots+b_nR_{i_n} = 0$$

where $0 \neq b_j \in Z$, R_{i_j} is a row of B_k, $j = 1,2,\ldots,n$ and $n < k$.

Since each column of B_k contains at most two nonzero elements a and $-a$

($a \in Z$) we see that for every b_j, there exists b_i such that $b_i = b_j$. Hence, we can rewrite the relation (**) in the form

$b_1 R_{j_1} + b_1 R_{j_2} + \ldots + b_m R_{j_{2m-1}} + b_m R_{j_{2m}} = 0$ with $j_{2k-1} < j_{2k}$, $k = 1,2,\ldots,m$.

At least one of the rows R_{j_1} or R_{j_2} contains a nonzero position other than $(j_1,(j_1,j_2))$ or $(j_2,(j_1,j_2))$. Let it be $(j_1,(j_1,j))$. If $R_j \notin \{R_{j_1},\ldots,R_{j_{2m}}\}$ then $b_1 = 0$ contradicting our assumption. Hence, $R_j \in \{R_{j_1},\ldots,R_{j_{2m}}\}$ and it follows that $b_1 = b_i$ for some $i \neq 1$. Repeating this argument we can finally conclude that all

coefficients in the relation (*) are equal to b_1. Since $n < k$ and B_k represents an equivalence class in the set of vertices, there exists a vertex $v_j \notin \{v_{i_1},\ldots v_{i_n}\}$ which is connected to at least one of the vertices $v_{i_1},\ldots,v_{i_n}$. Suppose that v_j is connected to v_{i_1}. This implies that in the column (i_1,j) when $i_1 < j$ or in the column (j,i_1) when $j < i_1$ the only nonzero positions are $(i_1,(i_1,j))$ and $(j,(i_1,j))$ in the first case or $(j,(j,i_1))$ and $(i_1,(j,i_1))$ in the second case. Thus, $b_1 = 0$ contradiciting our assumption.

<u>Hence, any k–1 rows of B_k are linearly independent, in particular</u>

<u>rank $(B_k) = k-1$.</u>

Let B_1 be the normal form of B, i.e., $B_1 = \text{diag.}\{d_1,\ldots,d_r,0,0\ldots0\}$ with $d_i \mid d_{i+1}$. Rank $(B(p)) = N-1$, for every p if and only if rank$(B_1(p)) = N-1$ for every p; i.e., if $r = N-1$ and $d_r = \pm 1$. Thus:

$G(p)$ is connected for every prime number p if and only if the greatest common divisor of the $N-1$–rowed minors of B is equal to 1.

<u>Example III.5.</u>

Let L be a free Lie algebra over Z on $\{\xi_1,\xi_2,\xi_3\}$ with $\xi_1 > \xi_2 > \xi_3$

a) Let $\alpha_1 = [\xi_3,[\xi_1,\xi_2]]$ and $\alpha_2 = [\xi_2,[\xi_1,\xi_3]]$

then in $U(L)\otimes_Z Z/pZ$ the highest terms $\hat{\alpha}_1 = -\xi_1\cdot\xi_2\cdot\xi_3$ and $\hat{\alpha}_2 = \xi_1\cdot\xi_2\cdot\xi_3$ are combinatorially free for all prime numbers p. Hence, they are strongly free for all p. Thus α_1 and α_2 are strongy free as elements of L.

b) let $\alpha_1 = [\xi_1,\xi_2]$ and $\alpha_2 = [[\xi_1,\xi_3],\xi_2]$.

Then, in $U(L)\otimes_Z Z/pZ$ the highest terms $\hat{\alpha}_1 = \xi_1\xi_2$ and $\hat{\alpha}_2 = \xi_1\cdot\xi_3\cdot\xi_2$ are combinatorially free for all p. Hence, α_1,α_2 are strongly free in L.

Note that we could conclude this directly from Proposition I.3.3 taking $\mathfrak{a}$ to be the ideal of L generated by ξ_1.

BIBLIOGRAPHY

1. Main references

[1] David J. Anick, Inert sets and the Lie algebra associated to a group (to appear).

[2] ________, Non-commutative graded algebras and their Hilbert series. J. Algebra, Vol. 78, No. 1, Sept. 1982, pp. 120–140.

[3] A. Bahturin, Identities in Lie algebras. Moscow, 1985 (Russian).

[4] N. Bourbaki, Lie groups and Lie algebras. Chapters 1 and 2, Herman, Paris, 1960.

[5] H. Cartan, S. Eilenberg, Homological Algebra. 1956, Princeton Math. Series, No. 14.

[6] Marshall Hall, Jr. A basis for free Lie rings and higher commutators in free groups. Proc. Amer. Math. Soc., 1 (1950), pp. 575–581.

[7] J. Labute, Algèbres de Lie et pro–p–groupes définis par une seule relation. Invent. Math, 4(1967), pp. 142–158, MR36 No.1581.

[8] ________, On the descending central series of groups with a single defining relation. J. Algebra, 14(1970), pp. 16–23, MR40 No. 4324.

[9] ________, The lower central series of the group $\langle x,y,:x^p=1\rangle$. Proc. Amer. Soc., 66, (1977), pp. 197–201, MR58, No. 903.

[10] ________, The determination of the Lie algebra associated to the lower central series of a group. Amer. Math. Soc., Vol. 288, No. 1, March 1985, pp. 51–57.

[11] ________, A note on a conjecture of Murasugi (to appear)

[12] W. Magnus, A. Karrass D. Silitar, Combinatorial group theory:

presentation of groups in terms of generators and relations. Pure and Appl. Math., Vol. 13, Interscience, New York, 1966, MR34, No. 7617.

[13] J.P. Serre, Lie algebras and Lie groups, 1964, Lectures given at Harvard University, Benjamin, New York, 1965.

[14] A.I. Sirsov, Subalgebras of free Lie algebras. Math. Sbornik, N.S. 33 (75), pp. 441–452, (1953) (Russian).

[15] E. Witt, Die Unterringe der freien Liescher Ringe. Math. Z. 64, (1956), pp. 195-216.

2. Other references

[16] A.I. Sirsov, Subalgebras of free commutative and free anticommutative algebras. Mat. Sbornik, N.S.34 (76), pp. 81–88, (1954) (Russian).

[17] W. Magnus, Ueber Gruppen und zugeordnete Liesche Ringe, J. Reine Angew. Math. (Crelle), 177, (1937) pp. 105–115.

[18] D. Quillen, On the associated graded ring of a group ring, J. Algebra 10, (1968), pp. 411–418.

[19] H.V. Waldinger, On extending Witt's formula. J. Algebra, 5, (1967), pp. 41–58.

[20] E. Witt, Treue Darstellung Liescher Ringe. J. Reine Angew. Math., 177, (1937), pp. 152–160.

[21] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie. Ann. Ecole Norm. sup., 71, (1954), pp. 101–190, MR19, No. 529.

[22] ________, Groupes analytiques p–adiques. Inst. Hautes Etudes Sci. Publ. Math., No. 26, (1965), pp. 389–603, MR35, No. 188.

[23] K.T. Chen, Commutator calculus and link invariants. Proc. Amer. Math.

Soc., 3, (1952), pp. 44–55.

[24] R.M. Hain, Iterated integrals, intersection theory and link groups. Topology, Vol. 24, (1985), No. 1, pp. 45–66.

[25] T. Maeda, Lower central series of link groups. Ph.D. thesis, University of Toronto (1983).

[26] W.S. Massey, L. Traldi, On a conjecture of K. Murasugi. Pacif. J. of Math., Vol. 124, No. 1, (1986), pp. 193–213.

[27] J. Milnor, Link groups. Annals of Math., Vol. 59, No. 2, (1954), pp. 177–195.