Lecture 2.

Let $X = \{x_i, i \in I\}$. We assume that the set of indices I is equipped with an order $<$, i.e. $\forall i, j \in I$ $i<j$ or $i=j$ or $j<i$, and

$i<j, j<k \Rightarrow i<k$.

Moreover, we assume that the order $<$ satisfies the minimality condition: there are no infinite descending chains

$i_1 > i_2 > \dots$

One of the forms of the Axiom of choice: on any nonempty set ~~we~~ there exists an order with minimality condition.

If $|X| < \infty$ then it is obvious.

Lexicographical order.

For $w = x_{i_1} x_{i_2} \cdots x_{i_p}$ and $v = x_{j_1} x_{j_2} \cdots x_{j_q}$

we say $w < v$ if

(i) $p < q$, or

(ii) $p = q$ and there exists k such

that $i_k < j_k$ with $i_1 = j_1, i_2 = j_2, \ldots, i_{k-1} = j_{k-1}$.

Example. $X = \{x_1, x_2, x_3\}$, $1 < 2 < 3$. Then

$$x_2 x_1 < x_1^3$$

$$x_2 x_3 x_1^2 < x_2 x_3 x_2 x_1$$

If $v' < v''$ then $uv'w < uv''w$,

where v', v'', u, w are words.

2. Free associative algebras.

Given a field F and a ~~to~~ nonempty set X we define $F\langle X\rangle$ to be the set of finite formal linear combinations of words from X^*. So, an element of $F\langle X\rangle$ looks like

$$\alpha_1 w_1 + \alpha_2 w_2 + \dots + \alpha_k w_k,$$

where $\alpha_i \in F$ and $w_1, \dots, w_k$ are distinct words from X^*.

We call $F\langle X\rangle$ the free associative F-algebra on X, where the operations extend linearly from the semigroup structure on X^*.

Clearly, X^* is a basis of the vectorspace $F\langle X\rangle$.

Why do we call this algebra a free algebra?

Proposition I.2.1. Let A be an associative F-algebra. An arbitrary mapping $X \xrightarrow{\varphi} A$ uniquely extends to an F-algebra homomorphism $\tilde{\varphi} : F\langle X \rangle \to A$.

Proof. By Proposition I.1.1 the mapping φ uniquely extends to a homomorphism $\overline{\varphi} : X^* \to A$ to the multiplicative semigroup of A. Extend $\overline{\varphi}$ linearly to all $F\langle X \rangle$. If

$$a = \sum_i \alpha_i w_i,$$

$\alpha_i \in F$; w_i are distinct words from X^*, then

$$\overline{\varphi}(a) = \sum_i \alpha_i \overline{\varphi}(w_i)$$

Since every element a is uniquely represented in the above form, the map is well-defined

Also, it is clear, that $\bar{\varphi}$ is the only such homomorphism. This completes the proof of the Proposition.

For an F-algebra A, suppose $\{a_i\}_{i \in I}$ is a generating set, i.e. every element of A can be represented ~~as a~~ (not necessarily uniquely) as a finite linear combination of products of a_i's.

Choose a set $X = \{x_i\}_{i \in I}$ to be an alphabet indexed by the same set I, so that we have the map $\varphi : X \to A$, $x_i \to a_i$, $i \in I$. Then Proposition I. 2. 1 guarantees that we have an algebra homomorphism $\bar{\varphi} : F\langle X \rangle \to A$.

Let $J = \ker \overline{\varphi}$, J is an ideal of $F\langle X\rangle$

In fact, since the image of $\overline{\varphi}$ is all of A, by the homomorphism theorem

$$A \cong F\langle X\rangle / J.$$

Let $R \subseteq J$ be a subset such that R generates J as an ideal. It means that J is the minimal ideal of $F\langle X\rangle$ containing the set R,

$$J = \{ \sum_i a_i r_i b_i \mid a_i, b_i \in F\langle X\rangle ; \; r_i \in R \}.$$

We say that $F\langle X\rangle / J$ ~~...~~ is the algebra <u>presented by generators X and relations</u> <u>R</u> and denote it as $F\langle X \mid R = 0\rangle$.

As noted before this algebra is isomorphic to the algebra A. We will call $F\langle X \mid R=0\rangle$ a presentation for A.

3. Groebner-Shirshov bases.

Given even a finite presentation $\langle x_1, \dots, x_m \mid r_1=0, \dots, r_n=0\rangle$ of an associative F-algebra it is difficult to say if two elements $a(x_1,\dots,x_m)$, $b(x_1,\dots,x_m) \in F\langle X\rangle$ are equal modulo the ideal $J = id_{F\langle X\rangle}(R)$. There exist finite presentations that defy any algorithm.

Now we will describe a class of finite presentations where such an algorithm exists. This method works not always, but often.

Let $f \in F\langle X \rangle$, $f = \alpha_1 w_1 + \dots + \alpha_n w_n$,

where $\alpha_1, \dots, \alpha_n \in F \setminus \{0\}$; $w_1, \dots, w_n$ are distinct ~~elements~~ words from X^*. Let

$$w_j = \max\{w_1, \dots, w_n\},$$

in the lexicographical order. We call w_j the <u>leading monomial</u> (leading word, leading term) of f and denote $w_j = \bar{f}$.

Let $A = F\langle X \mid R = 0 \rangle$. Then A is generated by elements $a_i = x_i + id_{F\langle X \rangle}(R)$. If $f \in R$ then $f(a_1, a_2, \dots) = 0$ in the algebra A. Hence

$$\bar{f}(a_1, a_2, \dots) = -\sum_{i \neq j} \frac{\alpha_i}{\alpha_j} w_i(a_1, a_2, \dots)$$

All words w_i, $i \neq j$, on the right hand side are smaller than $w_j = \bar{f}$, so $\bar{f}$, $f \in R$, can always be written as a linear combination of smaller words in the algebra A

__Def.__ A word $w \in X^*$ is called __reducible__ if it contains some $\bar{f}$, $f \in R$, as a subword, i.e. $w = w' \bar{f} w''$. Otherwise the word w is __irreducible__.

(see pp. 9.1-9.3)

__Proposition I. 3. 1.__ The algebra A is spanned by $w(a_1, a_2, \dots)$, where w runs over all irreducible words.

__Proof.__ An arbitrary element $a \in A$ has the form

$$a = \sum_i \alpha_i w_i(a_1, a_2, \dots).$$

If some word w_i contains $\bar{f}$, $f \in R$,

<u>Lemma I.3.1.</u> Let I be a set with an order $<$ that satisfies the minimality condition. Let $X = \{x_i, i \in I\}$. Then the set X^* with the lexicographical order also satisfies the minimality condition.

<u>Proof.</u> We need to show that X^* does not contain infinite strictly descending chain

$$w_1 > w_2 > \cdots \quad , w_i \in X^*.$$

Suppose that such a chain exists. Then

$$\text{length}(w_1) \geq \text{length}(w_2) \geq \cdots$$

This sequence stabilizes. Hence there exists $m \geq 1$ such that all words w_i, $i > m$, have the same length, n.

Replacing the sequence $w_1 > w_2 > \cdots$ by $w_{m+1} > w_{m+2} > \cdots$ we will assume that $\mathrm{length}(w_i) = n$ for all $i \geq 1$,

$w_i = x_{i1} x_{i2} \cdots x_{in}$, $x_{ij} \in X$. Again we have

$$x_{i1} \geq x_{i2} \geq \cdots$$

~~Since X sat~~ The set I and therefore the set X satisfy minimality conditions. Hence the sequence above stabilizes. Replacing the sequence $w_1 > w_2 > \cdots$ by a subsequence we will assume that all words $w_1, w_2, \cdots$ start with the same letter, i.e. $x_{11} = x_{21} = \cdots$

Consider the 2d letters. We have

$$x_{12} \geqslant x_{22} \geqslant x_{32} \geqslant \cdots$$

Again this sequence stabilizes, so passing to a subsequence we can assume that all 2d letters are equal, and so on.

At the n-th step we will get a sequence of equal words, a contradiction.

$w_i = w_i' \bar{f} w_i''$, then replace $\bar{f}$ by a linear combination of smaller words. Do it for every reducible word w_i. We will get a different presentation

$$a = \sum_j \beta_j \, v_j(a_1, a_2, \dots),$$

where

$$\max(v_1, v_2, \dots) < \max(w_1, w_2, \dots).$$

Do it again and again. The process can not be infinite since by Lemma I.3.1 X^* does not contain infinite lexicographically decreasing sequences. Hence at some point we will arrive at a presentation

$$a = \sum_k \gamma_k \, u_k(a_1, a_2, \dots),$$

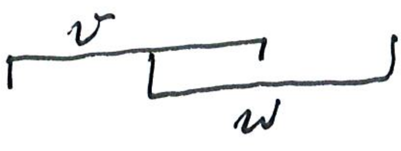
where all words u_k are irreducible.

this completes the proof of the Proposition

Note that this Proposition shows only that irreducible words span A and not that they form a basis of A. We would like a method determining when the latter is the case.

Given words $v, w \in X^*$ we say that <u>v, w admit a composition</u> if

(1) ~~one of the~~ the end of one of these words is a beginning of the other word



,

<u>Example</u> $v = x_1 x_2 \underbrace{x_3 x_1}, \; w = \underbrace{x_3 x_1} x_4 x_2,$

or

(2) one of these words is a subword of the other word

$$\underbrace{\quad \overbrace{\qquad}^{v} \quad}_{w}$$

Remark. Two words may admit more than one (but finitely many!) compositions.

$$u = x_1 x_2 x_1 x_2 \, , \quad v = x_2 x_1 x_2 x_2$$

$$w_1 = x_1 x_2 x_1 x_2 x_2 \, ,$$

$$w_2 = x_1 x_2 x_1 x_2 x_1 x_2 x_2$$

An arbitrary element in $F\langle X\rangle$ can be reduced to a linear combination of irreducible words via the algorithm in the proof of Prop. I.3.1.

R = set of defining relations.

$$f \in R, \quad f = \alpha \bar{f} + \sum_{v_i < \bar{f}} \alpha_i v_i, \; \alpha \neq 0.$$

<u>Reduction System</u>

$$\bar{f} = -\sum \frac{\alpha_i}{\alpha} v_i \quad , f \in R.$$

Of course, an element from $F\langle X\rangle$ can be reduced in many ways and to different linear combinations of irreducibles.

Reductions are equalities modulo $id(R)$.

<u>Ex.</u> $X = \{x, y, z\}$, $x < y < z$,

$$R = \{\underline{z^2} - xy - yx, \; \underline{zy} + yz - x^2\}$$

Reduction System

$$z^2 \to xy + yx$$
$$zy = -yz + x^2$$

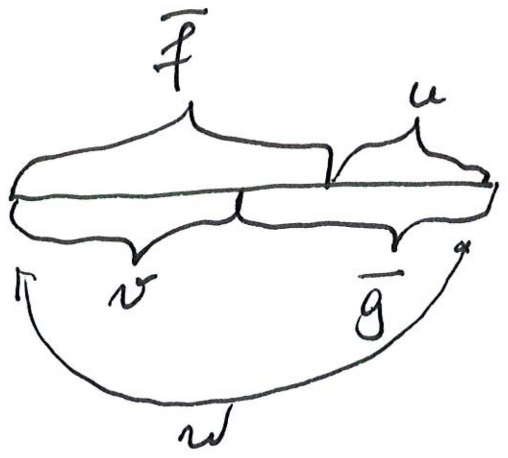
Reduce $z^2 y$.

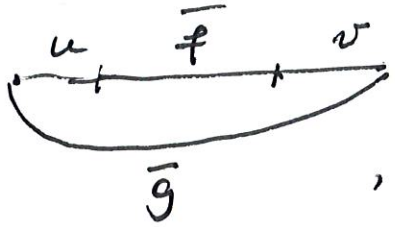
$$z^2 y \to (xy + yx)y = xy^2 + yxy$$

$$z(-yz + x^2) = -\underline{zy}z + zx^2 \to -(-yz + x^2)z + zx^2 = yz^2 - x^2 z + zx^2 = \boxed{\cancel{-yz^2 - x^2 z}}$$

$$\to y(xy + yx) - x^2 z + zx^2 = yxy + y^2 x - x^2 z + zx^2.$$

~~Let $A = F\langle X \mid R = 0 \rangle$~~ Let $f, g \in F\langle X \rangle$, the coefficients at $\bar{f}, \bar{g}$ respectively are equal to 1. Suppose that $\bar{f}, \bar{g}$ admit a composition



or 

, $w = \bar{g}$.

The element $(f,g)_w = fu - vg$ (resp. $(f,g)_w = ufv - g$) is called the composition of f, g with respect to the word w.

Let $A = F\langle X \mid R = 0\rangle$. Let Irr be the set of all irreducible words.

Theorem I.3.1. Irr is a basis of $F\langle X\rangle$ modulo $id_{F\langle X\rangle}(R)$ if and only if for any relations $f, g \in R$ that admit a composition these compositions $(f,g)_w$ reduce to 0.