Lecture 1

1. Polynomial Rings, Gröbner Bases

**Definition 1.1.** Let \( R \) be a ring, \( G \) an abelian semigroup, and \( R = \bigoplus_{i \in G} R_i \) a direct sum decomposition of abelian groups. \( R \) is **graded** \((G\text{-graded})\) if \( R_i R_j \subseteq R_{i+j} \) for all \( i, j \in G \). Similarly, let \( M = \bigoplus_{i \in G} M_i \) be an \( R \)-module. If \( R_i M_j \subseteq M_{i+j} \) for all \( i, j \in G \) then \( M \) is a **graded** \( R \)-module. \( M_i \) is called the \( i \)th graded homogeneous component of \( M \), and elements of \( M_i \) are called homogeneous elements of degree \( i \) or \( i \)th forms.

**Example 1.2.** Let \( k \) be a ring. Consider \( k[x] = \bigoplus_{n \in \mathbb{N}} kx^n \). Then \( k[x] \) is therefore \( \mathbb{N} \)-graded.

**Example 1.3.** Let \( k \) be a ring. Consider \( k[x,y] = \bigoplus_{(i,j) \in \mathbb{N}^2} kx^i y^j \), and this makes \( k[x,y] \) \( \mathbb{N}^2 \)-graded.

**Remark 1.4.** \( R_0 \) is a subring of \( R \), and \( R_0 \hookrightarrow R \) as a direct summand (show this!). Also, each \( R_i \) is a \( R_0 \)-module because \( R_0 R_i \subseteq R_i \). The same is true for \( M_i \), since \( R_0 M_i \subseteq M_i \).

**Definition 1.5.** Let \( M, N \) be graded \( R \)-modules, and \( \phi : M \rightarrow N \) where \( \phi \) is \( R \)-linear. Then \( \phi \) is **graded** of degree \( d \) (sometimes called homogeneous if \( d = 0 \)) if \( \phi(M_i) \subseteq N_{i+d} \) for all \( i \in G \). This gives the category of \( R \)-graded modules where the objects are graded \( R \)-modules and morphisms are graded homomorphisms of \( R \)-modules.

According to the definition, each \( x \in M \), where \( M \) is an \( R \)-graded module, can be written as a finite sum \( x = \sum x_i \), where each \( x_i \neq 0 \), and \( x_i \in M_i \). This is a unique representation and each \( x_i \) has degree \( i \in G \). By convention, 0 has arbitrary degree. We will call this expression the **graded decomposition** of \( x \).

This notion is of great importance in module theory. The grading helps to prove statements by keeping track of the grading.

**Definition 1.6.** Let \( R \) be a \( G \)-graded ring and \( M \) be an graded \( R \)-module. We say that a submodule \( N \) in \( M \) is graded (or homogeneous) submodule if \( x \in N \) with graded decomposition \( x = \sum x_i \), \( x_i \in M_i \) implies \( x_i \in N \) for all \( i \).
Proposition 1.7. Let $R$ be a $G$-graded ring and $M$ be an graded $R$-module. Then a submodule $N$ of $M$ is homogeneous if and only if it is generated by homogeneous elements.

Proof. Assume first that $N$ is a homogeneous submodule. Let $x$ be an elements from a list of generators of $N$. One can replace $x$ by its homegenous components in the generating set, and therefore, by doing this with every generator, one will obtain a homogenous generating set.

Conversely, let $N = <S>$ where $S$ is a set of homogenous elements for $N$.

Let $x \in N$ and write $x = \sum_{finite} r_i x_i$, $x_i \in S$. Note that we assume $deg(x_i) = i \in G$.

In the equality above look in degree $\alpha \in G$: $x_\alpha = \sum s_j x_j$ where $x_\alpha$ is the homogenous part of $x$ in its graded decomposition, and $s_j, x_j$ are homogeneous elements of degrees $k_j$ and $j$ such that $\alpha = k_j + j$, $x_j \in S$. Since $x_j$ are in $N$ it follows that $x_\alpha$ is in $N$ too. □

Let $\mathbb{N} = \{0,1,2,3,...\}$, the set of natural numbers. Let $k$ be a field, and $R = k[x_1,...,x_n]$ be the ring of polynomials in $n$ variables with coefficients in $k$. Let $f \in R$, so $f = \sum_{finite} a_\alpha x_\alpha$, where $x = x_1 \cdot x_2 \cdots x_n$, $\alpha = (\alpha_1,...,\alpha_n) \in \mathbb{N}^n$, $a_\alpha \in k$, and $a_\alpha \neq 0$. We use the notation $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Definition 1.8. A monomial in $R$ is an element of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x^\alpha$. If $M = x^\alpha$, then the multidegree of $M$ is $(\alpha_1,...,\alpha_n) \in \mathbb{N}^n$.

One should note that we have the following decomposition as a direct sum of $k$-vector spaces

$$R = \bigoplus_{\alpha \in \mathbb{N}^n} M_\alpha,$$

where for all $\alpha$, $M_\alpha = k x^\alpha$ is an one dimensional $k$-vector space with basis $\{x^\alpha\}$.

Note that $k \subset R$, and we customarily call an element of $k$ a constant of $R$.

1.1. Monomial Orderings. We have noticed that for 1 variable polynomials over a field, the notion of degree has allowed one to prove several important results, such as the PID property. An important feature of the degree notion is that it provides a total order on monomials with certain additional properties.
For $R = k[x_1, \ldots, x_n]$, $k$ field, we want to define an order on the monomials such that they totally ordered, and the order is preserved if monomials are multiplied by the same element. Also, we want comparability among all elements and to have a smallest element for a given subset.

**Definition 1.9.** A monomial ordering on $\mathbb{N}^n$ is an order relation $>$ such that:

1. $>$ is total (everything is comparable),
2. if $\alpha > \beta$, then $\alpha + \gamma > \beta + \gamma$ for all $\gamma \in \mathbb{N}^n$ (this is the compatibility with multiplication),
3. Every subset of $\mathbb{N}^n$ has a least element.

This monomial ordering on $\mathbb{N}^n$ induces an ordering on the monomials in $R = k[x_1, \ldots, x_n]$, with $k$ a field. A monomial has the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $x^\alpha \leq x^\beta$ if and only if $\alpha \leq \beta$. We obtain an order on the monomials of $R$ with an order relation $>$ such that it is a total order, it is additive, and every subset has a least element.

It is often assumed by many authors that $x_1 > x_2 > \cdots > x_n$, but this is not part of the definition. Also, for $n \leq 3$, $x, y, z$ are often used instead of $x_1, x_2, x_3$.

Consider the following three monomial orderings:

**Definition 1.10.** Let $\alpha, \beta \in \mathbb{N}^n$.

1. **Lexicographical Order (lex)**
   
   In this order, $x^\alpha > x^\beta$ if the leftmost nonzero entry of $\alpha - \beta$ is positive.
   
   For example, $x^2y >_{\text{lex}} xy^5z$ because $(2, 1, 0) - (1, 5, 1) = (1, -4, -1)$, and the leftmost entry is 1 which is positive. Also, $x^2y^3z >_{\text{lex}} x^2yz^8$ since $(2, 3, 1) - (2, 1, 8) = (0, 2, -7)$, and the leftmost nonzero entry, 2, is positive. Here, $x > y > z$.

2. **Graded Lexicographical Order (glex, hlex, grlex)**
   
   In this order, $x^\alpha > x^\beta$ if $\sum_i \alpha_i > \sum_i \beta_i$ or if $\sum_i \alpha_i = \sum_i \beta_i$ and $\alpha >_{\text{lex}} \beta$.
   
   For example, $x^2y^2z >_{\text{glex}} x^3y$, and $x^3yz >_{\text{glex}} x^2x^2z$. Here $x > y > z$.

3. **Graded Reverse Lex Order (grevlex)**
   
   In this order, $x^\alpha > x^\beta$ if $\sum_i \alpha_i > \sum_i \beta_i$ or if $\sum_i \alpha_i = \sum_i \beta_i$ and the rightmost nonzero entry of $\alpha - \beta$ is negative.
   
   For example, $x^3y^2z^5 < x^4y^6$, and $x^2y^2z^5 < xy^4z^4$. Also, $x > y > z$. 
**Remark 1.11.** The natural question is what about a reverse lex order (instead of graded reverse lex). This would be defined as $\alpha > \beta$ if the rightmost nonzero entry of $\alpha - \beta$ is negative. This is not a monomial ordering since there is no least element, i.e., consider $\{xy^a\}_a$. As $a$ increases, the corresponding monomial gets smaller and smaller without bound. There is no least element in this set.

Fix a monomial ordering on $R$, say >. Take $f \in R$. Then we write $f$ in a standard form such that the monomials appear in decreasing order, i.e., $f = a_\alpha x^\alpha + \cdots$.

**Definition 1.12.** We call $\alpha$ the **multidegree** of $f$, $x^\alpha$ the **leading monomial** of $f$, $a_\alpha$ the **leading coefficient** (LC) of $f$, and $a_\alpha x^\alpha$ the **leading term** (LT) of $f$.

Given a polynomial ring, we want to know how to divide two or more polynomials into another polynomial simultaneously. This is done with a division algorithm, after fixing a monomial ordering.

1.2. **Division Algorithm.** Fix a monomial ordering on $\mathbb{N}^n$ (and hence on $k[x_1, \ldots, x_n]$) and an ordered $m$-tuple $(g_1, \ldots, g_m)$ with $g_i \in R = k[x_1, \ldots, x_n]$ for every $i = 1, \ldots, m$.

The division algorithm allows us to claim that every $f \in R$ can be written as

$$f = a_1g_1 + \cdots + a_mg_m + r,$$

with $a_i \in R$, and either $r = 0$, or $r$ is a $k$-linear combination of monomials, none of which are divisible by LT($g_1$), ..., LT($g_m$). Moreover, if $a_ig_i \neq 0$, then the multidegree of $f$ is greater or equal to the multidegree of $g_i$ for all $i = 1, \ldots, m$.

We present now the division algorithm. Essentially, the algorithm allows us to simultaneously divide $f(x)$ by an ordered set of polynomials $\{g_1(x), \ldots, g_m(x)\}$. It proceeds as follows:

1. Compute LT($f$). If LT($g_1$)|LT($f$), then write $h = \frac{\text{LT($f$)}}{\text{LT($g_1$)}}$ and set $f = f_1 := f - hg_1$. Repeat with $f$ LT($g_1$) /LT($f$).
2. Move to $g_2$ and apply step 1 to $f$. If LT($g_2$)|LT($f_1$), then set $f_1 = f - hg_2$. Now start over with testing $g_1$ into $f_1$, and moving through (1) and (2) with the $g_i$s until some LT($g_j$) does not divide LT($f_1$). So for each new $f_k$ the algorithm starts again with $g_1$ and moves through to $g_i$, $i = 1, \ldots, m$. 
(3) At some point, no leading terms of any the $g_i$’s will divide $LT(f_k)$. Write $f = a_1g_1 + \cdots + a_mg_m + r$ where $LT(r)$ is not divisible by any of the $LT(g_i)$. Repeat the previous steps to $f_{k+1} = r - LT(r)$.

Example 1.13. Fix the lex monomial ordering on $k[x, y]$. We want to divide \{ $g_1 = y^2, g_2 = xy + 1$ \} into $f = x^2y + xy^2 + xy$, all taking place in $k[x, y]$. Since $LT(g_1)$ does not divide $LT(f)$ we move to $LT(g_2)$, and we write $f_1 = x^2y + xy^2 + xy - x(xy + 1) = xy^2 + xy - x$. Now we can go back to $g_1$ to get $f_2 = xy^2 + xy - x - xy^2 - xy - x$. The leading term of $g_1$ does not divide $x^2y$ so we move to $g_2$. We get $f_3 = xy - x - (xy + 1) = -x - 1$. Now neither of the $LT(g_i)$ divide $LT(f_3)$, so we work with $r = -x - 1$. Note that $LT(r)$ is not divisible by $LT(g_1), LT(g_2)$, so we stop here.

We obtain

$$f = xg_1 + (x + 1)g_2 - x - 1.$$

2. Monomial Ideals

Definition 2.1. Let $R = k[x_1, \ldots, x_n]$, where $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. An ideal $a \leq R$ is a monomial ideal if $\sum a_{\alpha}x^\alpha \in a \Rightarrow x^\alpha \in a$ for every $a_{\alpha} \neq 0$.

In other words, a monomial ideal is a homogeneous ideal of $R$ under the $\mathbb{N}^n$-grading.

If $a$ is a monomial ideal in $R$, we can set $A = \{ \alpha \mid x^\alpha \in a \} \subseteq \mathbb{N}^n$. Then $A$ has the property that $\alpha \in A$ if and only if $\alpha + \gamma \in A$ for every $\gamma \in \mathbb{N}^n$. This induces a correspondence between monomial ideals $a$ and sets $A \subseteq \mathbb{N}^n$ that satisfy the condition mentioned above.

Lemma 2.2. Assume $a = (x^\alpha \mid \alpha \in A)$. Then $x^\beta \in a$ if and only if $\exists \alpha \in A$ such that $x^\alpha | x^\beta$.

Proof. One direction is clear. Now let $x^\beta \in a$. Then

$$x^\beta = \sum_{i \in I} f_i x^{\alpha_i},$$

where the sum above is finite, $f_i \in R$ and $\alpha_i \in A$ for all $i \in I$. 
Two polynomials are equal if and only if they are equal in each multidegree. So in the above equality look in degree $\beta$. This will give

$$x^\beta = \sum_{j \in J} M_j x^{\alpha_j},$$

where $M_j$ are monomials, and $J \subseteq I$. This implies in particular that for all $j \in J$ $x^{\alpha_j} | x^\beta$.

\[
\square
\]

**Proposition 2.3.** Let $a$ be a monomial ideal. Then there exists $A \subset \mathbb{N}^n$ such that

$$a = (x^\alpha : \alpha \in A).$$

\textbf{Proof.} Write $a = (f_i : f_i \in R, i \in I)$, where $I$ is a possibly infinite set. By the definition of a monomial ideal, we have that every monomial that appears in $f_i$ belongs to $a$. So we can replace the set of generators $\{f_i\}_{i \in I}$ by the set of generators consisting of the monomials appearing in each $f_i$, $i \in I$. This proves the statement.

\[
\square
\]

**Theorem 2.4.** (Dickson) Any monomial ideal is generated by a finite set of monomials.

\textbf{Proof.} We will prove this by induction on the number of variables $n$ in $R$.

When $n = 1$, $R$ is a PID so the result is clear.

Let $a$ be a monomial ideal in $R = k[x_1, \ldots, x_n]$. By the Proposition above, since $a$ is generated by monomials so we can write $a = (x^\alpha : \alpha \in A)$.

For every $k \in A$, and $i = 1, \ldots, n$ let us write

$$a_{(i,k)} = (x = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_{i-1}^{\alpha_{i-1}} x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n} : x \cdot x_i + \in a).$$

These ideals are generated by monomials in $n - 1$ variables so by the induction hypothesis they must be finitely generated. Let us denote a finite generating set of monomials for them by $G_{(i,k)}$.

Now choose $\alpha \in A$, so $x^\alpha \in a$. Let $x^\beta \in a$. If $\beta_i \geq \alpha_i$ for all $i = 1, \ldots, n$ then $x^\alpha \mid x^\beta$. If not, then there exists $i$ such that $\alpha_i > \beta_i$. 
But then \( x^\beta = x \cdot x_i^{\beta_i} \) with \( x \in a_{(i, \beta_i)} \). So, there exists an element \( z \) in \( G_{(i, \beta_i)} \) such that \( z \mid x \), so \( z x_i^{\beta_i} \mid x^\beta \).

In conclusion a finite set of generators for \( a \) is given by \( x^\alpha \) and all products of the form 
\( z \cdot x_i^{\beta_i} \) where \( z \in G_{(i, \beta_i)} \) and \( \beta_i \leq \alpha_i, i = 1, \ldots, n \).

\[ \Box \]

**Theorem 2.5.** *(Hilbert Basis Theorem-special case)* Any nonzero ideal \( I \leq k[x_1, \ldots, x_n] \) can be generated by a finite set of elements.

**Proof.** Let \( \text{LT} (I) \) be the ideal generated by the leading terms of all \( f \in I \). Then by the Dickson lemma, \( \text{LT} (I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle \). Take \( f \in I \) and apply the division algorithm to \( f, (g_1, \ldots, g_s) \) to obtain 
\[ f = a_1 g_1 + \cdots + a_s g_s + r, \] and since \( r \in I \), then \( \text{LT} (r) \in \text{LT} (I) \). This implies that \( \exists k \) such that \( \text{LT}(g_k)|\text{LT}(r) \), a contradiction unless \( r = 0 \). So \( I = \langle g_1, \ldots, g_s \rangle \). \[ \Box \]

The set \( \text{LT}(g_1), \ldots, \text{LT}(g_s) \) that appeared in the proof of the Hilbert Basis Theorem proved to be an important tool in commutative algebra and we will formally introduce it now.

**Definition 2.6.** Fix a monomial ordering and consider an ideal \( a \leq R = k[x_1, \ldots, x_n] \). Then a finite set \( S = \{g_1, \ldots, g_s\} \subset a \) is a Gröbner basis (GB) for \( a \) if 
\[ \langle \text{LT}(g) : g \in a \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle. \]

**Theorem 2.7.** Any nonzero ideal \( a \) of \( R \) has a GB and this basis generates the ideal.

**Proof.** Exactly as for the Hilbert basis theorem, it is easy to see that \( a \) has a GB. Now if \( f \in a \), apply the division algorithm to obtain 
\[ f = a_1 g_1 + \cdots + a_s g_s + r. \] If \( r \neq 0 \) then \( r \in a \) implies \( \text{LT} (r) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_s) \rangle \), a contradiction. \[ \Box \]

It is important to realize that for an arbitrary set of generators for an ideal \( I \) their leading terms do not necessarily generate \( \text{LT}(I) \).

**Example 2.8.** Let \( g_1 = x^2 y + x - 2 y^2 \), \( g_2 = x^3 - 2 x y \), with respect to the grevlex order.
Then \( a = \langle g_1, g_2 \rangle \), and \( x^2 = x g_1 - y g_2 \in a \). So \( \langle \text{LT}(g_1), \text{LT}(g_2) \rangle = \langle x^2 y, x^3 \rangle \) which does not contain \( x^2 \).
**Proposition 2.9.** Let $S = \{g_1, \ldots, g_s\}$ be a GB for $a$. Then $\forall f \in R, \exists! r \in R$ such that $f = g + r$ for some $g \in a$ and no term of $r$ is divisible by any of the $LT(g_i)$’s.

**Proof.** For existence, use the division algorithm to get the $r$ so that $f = a_1g_1 + \cdots + a_sg_s + r$. Let $g = f - r$. For uniqueness, assume $f = g_1' + r_1 = g_2' + r_2$ for $g_1', g_2' \in a$. Then $r_2 - r_2 = -g_2' + g_1' \in a$. This implies $LT(r_2 - r_1) \in LT(a) = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Thus $LT(r_2 - r_1)$ is some monomial in $r_2$ or $r_1$, a contradiction. □

**Corollary 2.10.** With the same notation as above, $f \in a$ if and only if $r = 0$ when $f$ is divided by $S$.

With the definition above it is known that Gröbner bases are not unique for a given ideal. Therefore, we will refine the definition in order to obtain this property.

**Definition 2.11.** A GB $= \{g_1, \ldots, g_s\}$ is minimal if $LC(g_i) = 1$ and $LT(g_i) \notin (LT(g_j) \mid j \neq i)$.

Note that an ideal can admit infinitely many minimal GB’s, but it is a fact that all minimal GB bases for an ideal $a$ have the same cardinality.

**Definition 2.12.** A GB is reduced if $LC(g_i) = 1$ and for every $g_i \in GB$, no monomial appearing in $g_i$ is in $\langle LT(g_1), \ldots, LT(g_{i-1}), LT(g_{i+1}), \ldots, LT(g_s) \rangle$.

The following important fact is stated here without proof.

**Proposition 2.13.** Each nonzero ideal $a$ has a unique reduced GB with respect to a given monomial ordering.