Masterarbeit

Markus Müller

Inhaltsverzeichnis

KAPITEL 1

Basics of commutative algebra

1. Notations and motivation

We start with a chapter on basic constructions in commutative algebra. In this work, every ring $R = (R, +, \cdot)$ is assumed to be commutative and have a unity.

DEFINITION 1. Let R be a ring. A set M is called ***R-module*** if $(M, +)$ is an abelian group with a scalar multiplication $R \times M \to M$, $(r, m) \to r \cdot m$ satisfying

- $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m) \quad \forall r_1, r_2 \in R \, \forall m \in M$
- $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m \quad \forall r_1, r_2 \in R \, \forall m \in M$
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2 \quad \forall r \in R \, \forall m_1, m_2 \in M$

A ***submodule*** of M is a subset $N \subseteq M$ which is a R-module itself.

REMARK 1. Every ring R is a R-module, and every ideal I of a ring R is a R-module. In the case that $R = k$ is a field, M is a vector space.

The theory of modules is much harder than the theory of vector spaces. Indeed, a module does not have to possess a basis.
In the most cases, we will consider (polynomial) rings and ideals of rings. By regarding those as modules, we can apply the theory of modules to them.

DEFINITION 2. Let k be a field and $R = k[x_1, \ldots, x_n]$ be the polynomial ring.

(1) A ***grading*** on R is a function $\deg : \{x_1, \ldots, x_n\} \to \mathbb{N}/\{0\}$. R is called ***standard graded*** if $\deg \equiv 1$.
(2) A ***monomial*** of R is a product $x^\alpha := x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Given a grading, we define $\deg(x^\alpha) := \sum\limits_{k=1}^{n} \alpha_k \deg(x_k)$ as the ***degree*** of x^α.
(3) For a $p \in R$, we define $\deg(p)$ to be the highest degree of any term in the polynomial. The elements of degree 0 are exactly the elements of k. For computational reasons, $0 \in R$ has arbitrary degree.

(4) For a given $i \geq 0$, denote by R_i the vector space spanned by all monomials of degree i.
(5) A polynomial $p \in R$ is called ***homogeneous*** if all of its terms have the same degree. 0 is a homogeneous polynomial of any degree.

PROPOSITION 1. Let $R = k[x_1, \ldots, x_n]$ and R_i defined as above.
(1) For given $i, j \in \mathbb{N}$, $R_i R_j \subseteq R_{i+j}$.
(2) If $p, q \in R$ are homogeneous, $\deg(pq) = \deg(p) + \deg(q)$.
(3) Every $p \in R$ can be written uniquely as finite sum $\sum_{i \geq 0} p_i$ with $p_i \in R_i$.

BEWEIS. Trivial. □

REMARK 2. The unique p_i in the above proposition are called ***homogeneous components of degree*** i. By the proposition, they are well defined. We therefore get a decomposition $R = \bigoplus_{i \geq 0} R_i$, where R is regarded as a k-vector space.

2. Graded structures

DEFINITION 3. Let k be a field.
(1) A ring R is called ***graded ring*** if there exist abelian groups $\{G_i = (G_i, +); i \in \mathbb{N}\}$ satisfying $R = \bigoplus_{i \geq 0} G_i$ and $G_i G_j \subseteq G_{i+j}$ for all $i, j \in \mathbb{N}$.
(2) A R-algebra A is called ***graded algebra*** if it is graded as a ring.
(3) Let $R = \bigoplus_{i \geq 0} R_i$ be a graded ring. An R-module M is called ***graded module*** if there is a set of additive subgroups $\{M_i, i \in \mathbb{N}\}$ of $(M, +)$ satisfying $M = \bigoplus_{i \geq 0} M_i$ and $R_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{N}$.
(4) A R-submodule N of a graded module $M = \bigoplus_{i \geq 0} M_i$ is called ***graded submodule*** if

$$N = \bigoplus_{i \geq 0} N \cap M_i.$$

(5) An element of G_i resp. M_i is called ***homogeneous*** of degree i.

REMARK 3. If M is a graded R-module and M has the decomposition $M = \bigoplus_{i \geq 0} M_i$, the M_i are R-modules. In the case that $R = k$ is a field, the M_i are vector spaces. We will encounter this situation when we consider k-algebras.

EXAMPLE 1. Let R be a graded ring.

(1) Given a field k, the polynomial ring $k[x_1, \dots, x_n]$ is a graded $k[x_1, \dots, x_n]$-module.
(2) Direct sums of graded R-modules are graded R-modules again.
(3) R is a graded R-module.
(4) $R^n = R \oplus \cdots \oplus R$ (n times) is a graded R-module.
(5) If S is a multiplicatively closet subset of homogeneous elements of R, then the localization R_S is a graded ring.

3. Graded ideals

By considering ideals of rings, one may ask how the ideal may inherit the grading of the respective ring.

DEFINITION 4. Let R be a graded ring. An ideal I of R is called ***graded ideal*** if it is graded as a submodule of R.

PROPOSITION 2. Let M be a graded R-module and N be a R-submodule of $M = \bigoplus_{i \geq 0} M_i$. The following are equivalent

(1) N is a graded R-submodule of M.
(2) $N = \sum_{i \geq 0} N \cup M_i$.
(3) All homogeneous components of elements of N are in N.
(4) N is generated by homogeneous elements.

BEWEIS. <u>(1) ⇔ (2)</u>: Trivial, since $M = \bigoplus_{i \geq 0} M_i$.
<u>(2) ⇒ (3)</u>: The homogeneous components of elements of N are exactly those in the sets $N \cup M_i$.
<u>(3) ⇒ (4)</u>: N is generated by all homogeneous components of elements of N, since they are all in N.
<u>(4) ⇒ (2)</u>: Suppose $N = \langle n_j, j \in J \rangle_R$ where the n_j are homogeneous components and J is an index set. Then

$$\sum_{i \geq 0} N \cup M_i \subseteq N = \sum_{j \in J} R n_j \subseteq \sum_{i \geq 0} N \cup M_i.$$

□

REMARK 4. Let k be a field and $R = k[x_1, \dots, x_n]$ be the polynomial ring in over k in n indeterminates.

(1) It is well known that R is noetherian, s.t. every ideal of R is finitely generated, which follows from Hilberts basis theorem. Suppose that R is graded as defined in section 1. The graded ideals of R are exactly the ideals that are generated by a finite number of homogeneous polynomials in R, i.e. polynomials where each term has the same degree.
(2) Every monomial ideal (i.e. an ideal that is generated by monomials) of R is graded, since every monomial ideal is homogeneous.

Example 2. Suppose $R = \mathbb{Q}[x_1, x_2, x_3]$ and $\deg(x_i) = i$ for $i \in \{1, 2, 3\}$. Then R is graded via

$$R_i := \langle p \text{ monomial in } R, \deg(p) = i \rangle_{\mathbb{Q}}.$$

Therefore, the ideal $I := \langle x_2^3 - x_1^3 x_3 \rangle$ is graded, while $J := \langle x_2^3 - x_3^3 \rangle$ is not.

4. More on modules

4.1. Graded module homomorphisms.

Definition 5. Let M, N be R-modules. A map $f : M \to N$ is called a ***R-module homomorphism*** if

$$f(x+y) = f(x) + f(y),$$
$$f(rx) = rf(x)$$

for all $r \in R$ and all $x, y \in M$.

It is well known that compositions of R-module homomorphisms are again R-module homomorphisms and the set $\mathrm{Hom}(M, N)$ of R-module homomorphisms $M \to N$ is a R-module itself, where the operations $f + g$ and $r \cdot f$ are defined naturally.

Definition 6. Let $M = \bigoplus_{i \geq 0} M_i$ and $N = \bigoplus_{i \geq 0} N_i$ be graded R-modules and $f : M \to N$ be a R-module homomorphism.

(1) f is said to have ***degree*** i if $f(M_j) \subseteq N_{i+j}$ for all $j \geq 0$.
(2) The set of all homomorphisms $M \to N$ of degree i is denoted by $\mathrm{Hom}_i(M, N)$.
(3) A homomorphism $f : M \to N$ is called ***graded***, if $f \in \mathrm{Hom}_i(M, N)$ for some $i \in \mathbb{Z}$.

For computational reasons, graded homomorphisms of degree 0 are important, making the computation of dimensions easier. We therefore give an easy way to transform a graded homomorphisms of any degree to a degree 0 homomorphism.

Definition 7. Let $M = \bigoplus_{i \geq 0} M_i$ be a graded R-module. Define $M(-p)$ to be the graded R-module that is shifted by p degrees, i.e.

$$M(-p)_j = M_{j-p}.$$

In this definition, $M_j = 0$ for $j < 0$.

Suppose now that we are given a graded module homomorphism $f : M \to N$ of degree p. Then there exists a homomorphism $f' : M(-p) \to N$ of degree 0 with...

Example 3. Let $R = k[x_1, x_2, x_3]$ with grading $\deg(x_i) = i$ for $i \in \{1, 2, 3\}$ and A be the matrix $A := \begin{pmatrix} x_2^3 & x_3 \end{pmatrix}$.

(1) The homomorphism $R \oplus R \xrightarrow{A} R$ is not graded. Suppose we have a pair $(a, b)^T \in (R \oplus R)_i$, then $A \cdot (a, b)^T = ax_2^3 + bx_3 \notin R_j$ for all $j \in \mathbb{N}$.
(2) The homomorphism $R(-3) \oplus R \xrightarrow{A} R$ has degree 3 and is therefore graded. Suppose that $(a, b)^T \in (R(-3) \oplus R)_i$, then $A \cdot (a, b)^T = ax_2^3 + bx_3 \in R_{i+3}$.
(3) The homomorphism $R(-6) \oplus R(-3) \xrightarrow{A} R$ has degree 0 and is therefore graded. Suppose that $(a, b)^T \in (R(-3) \oplus R)_i$, then $A \cdot (a, b)^T = ax_2^3 + bx_3 \in R_i$.

4.2. The structure theorem for finitely generated graded modules. We want to show briefly that every finitely generated graded R-module is isomorphic with degree 0 to a quotient module M/M', where M is a finite sum of shifted R-modules and M' is a graded submodule of M.

Proposition 3. Let M be a graded R-module. Then there exists a system of homogeneous generators of M.

Beweis. Let G be a system of generators of M. By Proposition 2, all homogeneous components of all generators are in M themselves. Therefore, the set of all homogeneous components of elements of G generate M as a R-module. □

Proposition 4. Let M, N be graded R-modules and $f : M \to N$ be a graded homomorphism, and let $m \in M$ have the unique representation into homogeneous components $m = m_{a_1} + \cdots + m_{a_k}$. Then $f(m_{a_1}), \ldots, f(m_{a_k})$ are the homogeneous components of $f(m)$.

Beweis. We have

$$f(m) = f(m_{a_1}) + \cdots + f(m_{a_k}),$$

and since f is graded, $f(m_{a_i})$ is homogeneous for $1 \leq i \leq k$. □

PROPOSITION 5. Let $f : M \to N$ be a graded R-module homomorphism. Then $\ker(f) := \{m \in M : f(m) = 0\}$ is a graded submodule of M.

BEWEIS. Suppose that $m \in \ker(f)$ and m has the representation into homogeneous components $m = m_{a_1} + \cdots + m_{a_k}$. Then $0 = f(m_{a_1}) + \cdots + f(m_{a_k})$, and by Proposition 3, all of these summands are homogeneous, therefore 0. So $f(m_{a_1}), \ldots, f(m_{a_k}) \in \ker(f)$ and by Proposition 2, $\ker(f)$ is graded. □

Now we can state and prove the structure theorem.

THEOREM 1. Let $N = \bigoplus_{i \geq 0} N_i$ be a finitely generated graded R-module. Then there exists a graded isomorphism of degree 0 (i.e. a graded bijective homomorphsm) $f : N \to M/M'$, where M is a finite direct sum of shifted R-modules and M' is a graded submodule of N.

BEWEIS. Choose a (finite) system $\{n_1, \ldots, n_k\}$ of homogeneous generators of N and suppose $n_i \in N_{d_i}$ for $1 \leq i \leq k$. Set

$$M := R(-d_1) \oplus \cdots \oplus R(-d_k).$$

As a finite direct sum of graded R-modules, M is graded module. If 1 is the unity in R, the element $1 \in R(-d_i)$ has degree d_i, we call it e_i. The homomorphism

$$f' : M \to N, e_i \mapsto n_i$$

is a graded R-module homomorphism of degree 0. Chosing $M' = \ker(f)$ (which is graded as a submodule by Proposition 5), the isomorphy follows from the homomorphism theorem for modules.

□

4.3. Exact sequences.

DEFINITION 8. A sequence of R-modules and R-module-homomorphisms

$$\ldots \stackrel{f_{i-1}}{\to} M_{i-1} \stackrel{f_i}{\to} M_i \stackrel{f_{i+1}}{\to} M_{i+1} \stackrel{f_{i+2}}{\to} \ldots$$

is ***exact*** at M_i if $f_i(M_{i-1}) = \ker(f_{i+1})$. The sequence is called exact, if it is exact at every M_i.

There are some easy exact sequences, that only consist of only three nontrivial modules, namely the exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

where $f_1 : M_1 \to M_2$ is injective and $f_2 : M_2 \to M_3$ is surjective.

Given an exact sequence of R-modules

$$0 \overset{f_1}{\to} M_1 \overset{f_2}{\to} \cdots \overset{f_n}{\to} M_n \overset{f_{n+1}}{\to} 0,$$

we can decompose this sequence into n short exact sequences via

$$0 \to \ker(f_{i+1}) \to M_i \overset{f_{i+1}}{\to} \operatorname{Im}(f_{i+1}) \to 0$$

for $0 \leq i \leq n-1$.
On the other hand, given these n short exact sequences, one may merge them to a long one.

Definition 9. Let C be a category of R-modules. A map $\lambda : C \to \mathbb{Z}$ is called ***additive***, if for every short exact sequence of R-modules in C given by $0 \to M_1 \to M_2 \to M_3 \to 0$, we have $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$.

Example 4. Let C be the category of the finite dimensional vector spaces over a field k. Then $\lambda : C \to \mathbb{Z}, \lambda(M) = \dim_k M$ is an additive function.

Proposition 6. Let C be a category of R-modules and $\lambda : C \to \mathbb{Z}$ be an additive function. Suppose we are given an exact sequence

$$0 \overset{f_1}{\to} M_1 \overset{f_2}{\to} \cdots \overset{f_n}{\to} M_n \overset{f_{n+1}}{\to} 0,$$

where $M_i \in C$, then

$$\sum_{i=1}^{n} (-1)^i \lambda(M_i) = 0.$$

Beweis. Decomposing the exact sequence into short exact sequences $0 \to \ker(f_{i+1}) \to M_i \to \operatorname{Im}(f_{i+1})$ for $2 \leq i \leq n+1$. By the additivity of λ, ...

□

5. Gröbner Bases

Gröbner bases are certain generating systems for ideals of the polynomial ring $k[x_1, \ldots, x_n]$. Since this works main emphasis is not on Gröbner bases, we will omit the proofs (which can be found in every standard book about commutative algebra).

5.1. Monomial order.

Definition 10. A ***monomial order*** on $R = k[x_1, \ldots, x_n]$ is a relation $\prec$ on $\mathbb{N}^n$ satisfying

(1) a well-order, i.e. a total order on R where every nonempty subset has a smallest element,

(2) $\alpha \prec \beta \Rightarrow \alpha + \gamma \prec \beta + \gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{N}^n$.

To an element $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ we can always consider the monomial $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. It is therefore suited to call such an order monomial.

EXAMPLE 5. (1) The relation $\prec_{\text{lex}}$ on $\mathbb{N}^n$ is defined by

$\alpha \prec_{\text{lex}} \beta :\Leftrightarrow$ the leftmost coordinate of $\alpha - \beta$, which is not 0, is negative.

This is a monomial order on $\mathbb{N}^n$, called *lexicographic order.*

(2) The relation $\prec_{\text{deglex}}$ on $\mathbb{N}^n$ is defined by

$$\alpha \prec_{\text{deglex}} \beta :\Leftrightarrow \sum_{i=1}^{n} \alpha_i \leq \sum_{i=1}^{n} \beta_n \text{ or } \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_n \text{ and } \alpha \prec_{\text{lex}} \beta.$$

This is a monomial order on $\mathbb{N}^n$, called *graded lexicographic order.*

Given a monomial order $\prec$ on $\mathbb{N}^n$, every polynomial has a unique term that is bigger than the other terms with respect to the chosen monomial order. The next definition is therefore well-defined.

DEFINITION 11. Denote by p a polynomial in $k[x_1, \ldots, x_n]$ with $p = \sum_{\alpha \in \mathbb{N}^n} p_\alpha x^\alpha$ and let $\prec$ be a monomial order on $\mathbb{N}$.

(1) The ***multidegree*** $\text{mdeg}(p)$ of p is defined as $\max(\alpha : p_\alpha \neq 0)$.
(2) The ***leading monomial*** $\text{LM}(p)$ of p is $x^{\text{mdeg}(p)}$.
(3) The ***leading coefficient*** $\text{LC}(p)$ of p is $p_{\text{mdeg}(p)}$.
(4) The ***leading monomial*** $\text{LT}(p)$ of p is $LC(p) \cdot LM(p)$.

5.2. The division algorithm on $k[x_1, \ldots, x_n]$. It is well known that there is a division algorithm on $K[x_1]$ with the lexicograpic order on $\mathbb{N}$. We will construct a similar division algorithm on $k[x_1, \ldots, x_n]$. Let p be a polynomial in $R := k[x_1, \ldots, x_n]$ and let $p_1, \ldots, p_k$ be given polynomials in R. We are interested in descriptions of p in the form

$$p = p_1 q_1 + \ldots p_k q_k + r,$$

where $q_1, \ldots, q_k, r \in R$. Clearly, this representation does not have to be unique (even if we want r to fulfil certain criterions).

PROPOSITION 7. Let $\prec$ be a monomial order on $\mathbb{N}^n$ and $p, p_1, \ldots, p_k$ be given polynomials in $R := k[x_1, \ldots, x_n]$. Then there exist $q_1, \ldots, q_k, r \in R$ with $p = p_1 q_1 + \ldots p_k q_k + r$ and no term of r is divisible by any leading term of $p_1, \ldots, p_k$.

BEWEIS. This theorem is very intuitive. For a proof and the corresponding algorithm, see XXXXX. □

Note that the $q_1, \ldots, q_k, r$ need not be unique.

Gröbner Basen fortfahren

KAPITEL 2

Dimension Theory

1. The Hilbert function and the Hilbert series

Given a graded structure, it is a natural question to ask questions on the nature of the graded components. For a graded ring, these components are abelian groups. In the case of a graded k-algebra, these components are not only abelian groups, but also k-vector spaces.

Definition 12. Let $S = \bigoplus_{i \geq 0} S_i$ be a finitely generated graded k-algebra. We define the ***Hilbert function*** Hilb_S by

$$\mathrm{Hilb}_S : \mathbb{N} \to \mathbb{N}, \quad i \mapsto \dim_k S_i.$$

In this definition, the S_i are regarded as vector spaces, making the definition well-defined. In the case of graded R-modules, the graded components need not be vector spaces, since we are not working over a field. We will adress this problem later. However, for the most cases, it will suffice to consider graded k-algebras. Furthermore, in the case of S not being finitely generated, we may have infinite dimensional components, which we want to exclude.

Definition 13. Let $S = \bigoplus_{i \geq 0} S_i$ be a finitely generated graded k-algebra. The ***Hilbert series*** $\mathrm{HilbS}_S(t)$ of S is the generating function of the dimensions of the S_i, i.e.

$$\mathrm{HilbS}_S(t) = \sum_{i \geq 0} \mathrm{Hilb}_S(i)\, t^i.$$

Example 6. Let $S := k[x, y, z]$. We will inspect the Hilbert function of S for different gradings.

- Suppose that S is standard graded. The S_i are generated by the monomials of degree i. The number of monomials of degree i is equal to the number of compositions of i into 3 parts (i.e. number of solutions $(a, b, c) \in \mathbb{N}^3$ with $a + b + c = i$), which is $\binom{i+2}{i}$. Therefore $\mathrm{Hilb}_S(i) = \binom{i+2}{i}$ and

$$\mathrm{HilbS}_S(t) = \sum_{i \geq 0} \binom{i+2}{i} t^i = \frac{1}{(1-t)^3}.$$

This is no coincidence, as we will see later in this chapter.

- Suppose that S is graded via $\deg(x) = 2, \deg(y) = 2, \deg(z) = 2$. Then the Hilbert series is given by

$$\mathrm{HilbS}_S(t) = \sum_{i \geq 0} \binom{i+2}{i} t^{2i} = \frac{1}{(1-t^2)^3}.$$

- Suppose that S is graded via $\deg(x) = 1, \deg(y) = 2, \deg(z) = 3$. The number of monomials of degree i is equal to the number of partitions of i into parts $1, 2$ and 3 (i.e. the number of non-decreasing sequences $(\lambda_k)_{k=1}^m$ with $\lambda_j \in \{1, 2, 3\}$ for $1 \leq j \leq m$ and $\sum_{k=1}^{m} \lambda_k = i$ for some m in $\mathbb{N}$). By elementary combinatorics, we conclude that

$$\mathrm{HilbS}_S(t) = \frac{1}{(1-t)(1-t^2)(1-t^3)}.$$

Because of the last example, the following proposition is easy to prove.

Proposition 8. Let $S := k[x_1, \ldots, x_n]$ with grading $\deg(x_i) = d_i$ for $1 \leq i \leq n$. Then

$$\mathrm{HilbS}_S(t) = \frac{1}{(1-t^{d_1}) \cdot \cdots \cdot (1-t^{d_n})}.$$

Those examples give the impression that studying Hilbert functions is quite easy. However, for I being a homogeneous ideal of $k[x_1, \ldots, x_n]$, computing the Hilbert series of $k[x_1, \ldots, x_n]/I$ is a nontrivial problem. We will get back to this problem in chapter 3. Hilberts Theorem gives us the nature of those Hilbert series.

Theorem 2. (Hilbert) Let $S := k[x_1, \ldots, x_n]$ graded via $\deg(x_i) = d_i$ and $M = \bigoplus_{i \geq 0} M_i$ be a finitely generated graded S-module. In this setting, the M_i are vector spaces. The Hilbert series of M is rational, and there exists a polynomial $p(t) \in \mathbb{Z}[t]$ satisfying

$$\mathrm{HilbS}_M(t) = \frac{p(t)}{(1-t^{d_1}) \ldots (1-t^{d_n})}.$$

BEWEIS. Induction on n. For $n = 0$, M is a vector space and $\mathrm{HilbS}_M(t)$ is a polynomial.
Suppose the claim holds for all finitely generated graded $k[x_1, \ldots, x_{n-1}]$-modules. The multiplication with x_n is a S-module-homomorphism $M_j \to M_{j+d_n}$ for all j, it is even a vector space homomorphism.

□