Combinatorics

Lecture Notes
Universität Leipzig

Summer 2024

Rainer Sinn

Version of April 28, 2024

Contents

Chapter 1: Introduction

Note that the class starts in the third week. First meeting is on April 15!

In this class, we will focus on combinatorics as the field of counting things. This is a vast area with many different methods and perspectives. After a brief introduction to some basic techniques, the main focus of the class is on Stanley-Reisner algebras/rings/ideals. This is an algebraic tool that can be used to prove properties of certain counts in the context of simplicial complexes. So essentially, we will introduce abstract simplicial complexes and study them with algebraic tools. They appear in nature in discrete geometry (e.g. the **boundary complex** of a simplicial polytope and more generally simplicial spheres) and algebraic topology (keyword **simplicial homology**), among other fields of mathematics.

One main point of Stanley-Reisner theory is to connect counts for simplicial complexes with algebraic invariants in the language of modules over polynomial rings. We will see Betti numbers and graded algebras. Abstract algebra is therefore a prerequisite, basics in commutative algebra are very useful, and familiarity with computer algebra systems (e.g. Macaulay2 or singular, the latter available in OSCAR) helps with computing examples.

The main sources for this course are the following.

Bibliography

[A] M. Aigner. A Course in Enumeration. *Graduate Texts in Mathematics*, Springer, 2007.

[HH] J. Herzog, T. Hibi. Monomial Ideals. *Graduate Texts in Mathematics*, Springer, 2011.

[MS] E. Miller, B. Sturmfels. Combinatorial Commutative Algebra. *Graduate Texts in Mathematics*, Springer, 2005.

Chapter 2: Combinatorics – the art of counting

Note that the class starts in the third week. First meeting is on April 15!

In *Enumerative Combinatorics* – also known as the art of counting – the goal is to systematically count the number of elements in a (countable) family of finite sets defined by combinatorial conditions. As a basic example, we might be interested to count the number of all 2-element subsets of the set $[n] = \{1, 2, \ldots, n\}$ of all positive integers up to n for any $n \in \mathbb{N}$. (Of course, the answer would be $\binom{n}{2}$.) Formally, we have an infinite family S_n of finite sets indexed by a typically infinite set I (for example, $n \in \mathbb{N}$) and we record the cardinality of S_n in a **counting function** $f\colon I \to \mathbb{N}_0$, $f(i) = |S_i|$. The index set I might also live in $\mathbb{N} \times \mathbb{N}$, for instance. In this first chapter, we introduce some basic ways to give answers to such questions. The notion of a generating function is the main point. This chapter is based on [A]. There are many more examples and interesting results in that book.

2.1. Generating Functions

The idea of generating functions is very simple but surprising useful. We give a short introduction based on [A, Sections 2 and 3].

Definition. A function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$ can be encoded in terms of a formal power series called the **generating function** of f defined simply as

$$F(z) = \sum_{i=0}^{\infty} f(i) z^i.$$

This is a formal power series in the sense that we consider it as an algebraic object in the ring $\mathbb{C}[[z]]$ of power series as opposed to an analytic object (essentially, we are not concerned with matters of convergence). The algebraic operations are defined as usual, namely

$$\sum_{i=0}^{\infty} a_i z^i + \sum_{j=0}^{\infty} b_j z^j = \sum_{i=0}^{\infty} (a_i + b_i) z^i \text{ and}$$
$$\sum_{i=0}^{\infty} a_i z^i \cdot \sum_{j=0}^{\infty} b_j z^j = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) z^k.$$

Simple rational functions correspond to power series (by taking their Taylor expansion around 0). We might use the following with convention $\binom{m}{i} = 0$ for

$i > m$.

$$\begin{aligned}
\frac{1}{1-z} &= \sum_{i=0}^{\infty} z^i \\
\frac{1}{1+z} &= \sum_{i=0}^{\infty} (-1)^i z^i \\
\frac{1}{1-z^2} &= \sum_{i=0}^{\infty} z^{2i} \\
(1+z)^m &= \sum_{i=0}^{\infty} \binom{m}{i} z^i \\
\frac{1}{(1-z)^m} &= \sum_{i=0}^{\infty} \binom{m+i-1}{i} z^i \\
\frac{z^m}{(1-z)^{m+1}} &= \sum_{i=0}^{\infty} \binom{i}{m} z^i
\end{aligned}$$

2.1.1 Exercise. Verify the expansions of rational functions as formal power series listed above.

2.1.2 Exercise. What are the units of the ring $\mathbb{C}[[z]]$ of formal power series (with respect to the above product)?
Hint: If you know what a discrete valuation ring is, this should lead you to the answer. Otherwise, analysis courses often give the answer as well (in which case you want to think of the power series as a convergent power series for intuition).

2.1.3 Exercise. Let A and B be two formal power series in $\mathbb{C}[[z]]$. Show that we get a well-defined series $A(B(z))$ if

(1) A is a polynomial, or
(2) the constant term of B is 0.

Furthermore, suppose that $A = \sum a_i z^i$ with $a_0 = 0$. Show that there exists a unique series $B = \sum b_j z^j$ with $b_0 = 0$ and $A(B(z)) = B(A(z)) = z$ if and only if $a_1 \neq 0$.

We might use the following series from analysis.

$$\begin{aligned}
\exp(z) &= \sum_{k=0}^{\infty} \frac{1}{k!} z^k \\
\log(1+z) &= \sum_{k=0}^{\infty} \frac{(-1)^{k+1}}{k} z^k \\
-\log(1-z) &= \sum_{k=0}^{\infty} \frac{1}{k} z^k
\end{aligned}$$

Sometimes it is useful to consider weights in addition to the counting function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$ (called Q-series in [A, Section 2.2]). Here is the primary example.

Definition. For a function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$, the **exponential generating function** is defined as

$$\widehat{F}(z) = \sum_{k=0}^{\infty} \frac{1}{k!} f(k) z^k.$$

As an example of the usefulness of exponential generating functions, prove the binomial inversion formula.

2.1.4 Exercise. Let $\widehat{A}(z) = \sum (a_i/i!) \cdot z^i$ and $\widehat{B}(z) = \sum (b_i/i!) \cdot z^i$ be two exponential generating functions for counting functions $a, b\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$. First, show that the equality $\widehat{B}(z) = \widehat{A}(z)\exp(z)$ is equivalent to

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$$

for all n. From this, derive the *binomial inversion formula* which says that the following two identities are equivalent:

$$\begin{aligned} b_n &= \sum_{k=0}^{n} \binom{n}{k} a_k \text{ for all } n \in \mathbb{Z}_{\geq 0} \\ a_n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k \text{ for all } n \in \mathbb{Z}_{\geq 0}. \end{aligned}$$

We will also consider the derivative of a formal power series as a formal, linear operation.

Definition. The **formal derivative** of $F(z) = \sum_{i=0}^{\infty} a_i z^i \in \mathbb{C}[[z]]$, denoted $F'(z)$ is defined as

$$F'(z) = \sum_{i=0}^{\infty} (i+1) a_{i+1} z^i.$$

2.1.5 Exercise. Show that familiar rules for derivatives also hold for formal derivatives of formal power series, i.e. show $(F+G)' = F' + G'$, $(FG)' = F'G + FG'$, $(F^{-1})' = -F'/F^2$, and $F(G(z))' = F'(G(z))G'(z)$, whenever the expressions are defined.

The formal derivative can be used to derive recursion formulas, for instance.

2.1.6 Example. Set $A(z) = \sum_{i=0}^{\infty} \binom{2i}{i} z^i$ and $a_i = \binom{2i}{i}$. By definition of binomial coefficients, we have

$$a_i = \binom{2i}{i} = \frac{2i(2i-1)}{i^2} a_{i-1}$$

so that $ia_i = 4ia_{i-1} - 2a_i$. This is equivalent to the formal identity

$$F' = 4(zF)' - 2F = 4zF' + 2F.$$

Now we use some tricks. First, we rewrite the identity as $F = \frac{1}{2}(1-4z)F'$. Second, we solve this using logarithms, namely

$$(\log(F))' = \frac{F'}{F} = \frac{2}{1-4z} = -\frac{1}{2}(\log(1-4z))'.$$

Integrating this identity (which we can again do formally, termwise), we get $\log(F) = -\frac{1}{2}\log(1-4z)$ – we don't have to worry about constant terms. Using the usual logarithmic exponential rule (exercise: this applies also in the setup of formal power series), we finally see

$$F(z) = \sum_{i=0}^{\infty} \binom{2i}{i} = \frac{1}{\sqrt{1-4z}}.$$

Exercise: Show, by Taylor expansion on the right hand side (or better yet of the identity $F^2 = 1/(1-4z)$), that this implies for all $n \geq 1$ the identity

$$\sum_{k=0}^{n} \binom{2k}{k}\binom{2(n-k)}{n-k} = 4^n.$$

2.1.7 Exercise. Find the unique sequence $(a_n)_{n\geq 0}$ of real numbers such that

$$\sum_{k=0}^{n} a_k a_{n-k} = 1$$

for all $n \geq 0$.

Another basic application of generating functions is to recursively defined sequences. The main result is the following.

2.1.8 Theorem. *Let $c_1, \ldots, c_d$ be a sequence of complex numbers for some integer $d \geq 1$ with $c_d \neq 0$ and set $c(z) = 1 + c_1 z + \ldots + c_d z^d \in \mathbb{C}[z]$. Denote by $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ the distinct roots of the reciprocal polynomial $c^R(z) = z^d c(\frac{1}{z})$ (in some order) so that*

$$c(z) = (1-\alpha_1 z)^{d_1} \cdots (1-\alpha_k z)^{d_k}$$

for multiplicities $d_i \in \mathbb{N}$. Let $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$ be a function. The following statements are equivalent.

(1) The function f satisfies the recurrence

$$f(n+d) + c_1 f(n+d-1) + \ldots + c_d f(n) = 0$$

of order d for all $n \geq 0$.

(2) The corresponding generating function is a rational function, namely there is a polynomial $p \in \mathbb{C}[z]$ of degree less than d such that

$$F(z) = \sum_{i=0}^{\infty} f(i) z^i = \frac{p(z)}{c(z)}.$$

(3) There are polynomials $p_i \in \mathbb{C}[z]$ of degree less than d_i ($i \in [k]$) such that

$$f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n.$$

Proof. The following sketches the main steps in the proof. See [A, Theorem 3.1] for full details. The proof is based on linear algebra, comparing vector spaces of dimension d over $\mathbb{C}$. We set

$$\begin{aligned} V_1 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon f(n+d) + c_1 f(n+d-1) + \ldots + c_d f(n) = 0 \text{ for all } n \geq 0\} \\ V_2 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon \sum_{i=0}^{\infty} f(i) z^i = \frac{p(z)}{c(z)} \text{ for some } p \in \mathbb{C}[z]_{d-1}\} \\ V_3 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n \text{ for some } p_i \in \mathbb{C}[z]_{d_i-1}\} \end{aligned}$$

with each vector space corresponding to one statement of the theorem. The first observation is that all three vector spaces have dimension d over $\mathbb{C}$. In the first case, we have d initial conditions; in the second, the polynomial p has d coefficients; and in the third, the polynomials p_i have d coefficients in total. Therefore, it suffices to prove inclusions of these vector spaces to conclude equality and therefore the theorem. The inclusion $V_2 \subset V_1$ is direct by comparing coefficients of the formal power series $c(z) \sum_{i=0}^{\infty} f(i) z^i = p(z)$; so we have $V_1 = V_2$. Finally, to show $V_1 = V_2 \subset V_3$, we use partial fraction decomposition of the rational function $p(z)/c(z)$ to obtain the polynomials p_i. Since the polynomials $(1 - \alpha_i z)^{d_i}$ divide $c(z)$, we can write

$$\frac{p(z)}{c(z)} = \sum_{i=1}^{k} \frac{g_i(z)}{(1-\alpha_i z)^{d_i}}.$$

Now we need to work a bit and manipulate this algebraically. The important result is the equality

$$\frac{g_i(z)}{(1-\alpha_i z)^{d_i}} = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{d_i - 1} \alpha_i^{-j} \cdot g_{i,j} \cdot \binom{n + d_i - j - 1}{d_i - 1} \right) \alpha_i^n z^n$$

where $g_i = \sum_{j=0}^{d_i-1} g_{i,j} z^j$. Comparing coefficients, we can read off the polynomials $p_i(n) = \sum_{j=0}^{d_i-1} \alpha_i^{-j} \cdot g_{i,j} \cdot \binom{n+d_i-j-1}{d_i-1}$ with the property that $f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n$ as claimed in (3). ∎

2.1.9 Exercise. Use the above result to give a closed formula for the nth Fibonacci number defined by the recurrence $F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$ of order 2 with initial conditions $F_0 = 0$ and $F_1 = 1$. (The golden ratio should appear in your computations.) What happens if we change the initial conditions? For instance, can you quickly adapt the solution to $F_0 = 10$ and $F_1 = -5$?

Chapter 3: Basics in commutative algebra

3.1. Noetherian rings and modules

In this section, we discuss some basics in abstract and commutative algebra. A ring R for us here is a commutative ring with unit which means that $(R, +)$ is an abelian group, $(R, \cdot)$ is associative, commutative, and has a neutral element $1 \in R$, and addition and multiplication are distributive. We will assume that $0 \neq 1$ (so the neutral element for addition and multiplication are distinct). Most commonly, we will work with polynomial rings $R = [x_1, \ldots, x_n]$. Another good example to keep in mind is $R = \mathbb{Z}$.

3.1.1 Exercise. Show that a ring R with $0 = 1$ is $R = \{0\}$.

Definition. Let R be a ring. A subset $I \subset R$ is an **ideal** of R if is is non-empty and satisfies $I + I \subset I$ and $R \cdot I \subset I$.

3.1.2 Exercise. Show that every ideal is an abelian group with respect to addition (inherited from R).

3.1.3 Proposition. *The intersection of ideals of a ring is again an ideal. In particular, for any set $M \subset R$, there is a unique smallest ideal containing M which we denote by $\langle M \rangle = \bigcap_{I \supset M} I$. We have*

$$\langle M \rangle = \left\{ \sum_{i=1}^{r} f_i g_i \mid r \in \mathbb{N}, f_i \in R, g_i \in M \right\}.$$

Proof. Exercise. ∎

3.1.4 Theorem. *Let k be a field and $R = k[x]$ be the polynomial ring over k in one variable x. Then every ideal of R is generated by one element.*

Proof. This follows from polynomial division with remainder. In other words, the ring R is **Euclidean**. Let $I \subset R$ be an ideal, $I \neq \{0\}$. Then there is a unique monic polynomial $f \in I$ of smallest degree (so with leading coefficient 1). Indeed, let f be any monic polynomial of smallest degree and pick $g \in I$. By polynomial division, we can write

$$g = q \cdot f + r$$

with $0 \leq \deg(r) < \deg(f)$ or $r = 0$. Since the degree of f is minimal over all elements in I and $r = g - q \cdot f \in I$, we must have $r = 0$ so that f divides g. ∎

3.1.5 Exercise. Let k be a field and $f, g \in k[t]$ be polynomials. (You can also start with $R = \mathbb{Z}$ – the arguments are similar.) Show that $\langle f \rangle + \langle g \rangle = \langle \gcd(f, g) \rangle$ (using the Euclidean algorithm). Also show that $\langle f \rangle \cap \langle g \rangle = \langle \operatorname{lcm}(f, g) \rangle$. Use this to find an example such that $\langle fg \rangle \subsetneq \langle f \rangle \cap \langle g \rangle$.

Definition. A **module** M over a ring R (or R-**module**) is an abelian group $(M, +)$ together with a scalar multiplication $R \times M \to M$, $(a, m) \mapsto a \cdot m$ satisfying the distributive laws $a(x + y) = ax + ay$ and $(a + b)x = ax + bx$, the associative law $(ab)x = a(bx)$, and the normalization $1x = x$.

3.1.6 Example. (1) For any ring R and any $n \in \mathbb{N}$, the n-fold direct product R^n is an R-module with componentwise scalar multiplication (analogous to the vector space k^n of column vectors for a field k).

(2) Any ideal of a ring R is an R-module. In fact, the ideals of R are exactly the R-modules contained in R.

(3) The $\mathbb{Z}$-modules are precisely the abelian groups.

(4) The trivial module over any ring R is $M = \{0\}$.

Definition. A **submodule** of an R-module M is a subgroup $U \subset M$ that is closed under scalar multiplication.

3.1.7 Exercise. Show that a subset $U \subset M$ of an R-module M is a submodule if and only if $U \neq \emptyset$, $U + U \subset U$, and $R \cdot U \subset U$.

3.1.8 Proposition. *Let M be an R-module. For any submodules U and V of M, the set*

$$(U : V) = \{a \in R \mid aV \subset U\}$$

is an ideal of R.

Proof. Exercise. ∎

3.1.9 Exercise. What is $(U : V)$ if $R = k$ is a field and M is a (say finite-dimensional) vector space over k?

Definition. The **annihilator** of an R-module M is the ideal

$$\operatorname{Ann}(M) = (\{0\} : M) = \{a \in R \mid ax = 0 \text{ for all } x \in M\}.$$

3.1.10 Exercise. Let R be a ring and $I \subset R$ an ideal. Show that $M = R/I$ is an R-module (with scalar multiplication $(a, \overline{x}) \mapsto \overline{ax}$) and compute the annihilator of M. (For simplicity, it might be good to start with $R = \mathbb{Z}$ and $I = \langle m \rangle$.)

3.1.11 Exercise. Let R be a ring and M be an R-module. Show the following claims.

(1) For any ideal $I \subset R$ contained in $\operatorname{Ann}(M)$, the module M is an R/I-module with scalar multiplication $\overline{a}x = ax$.

(2) The annihilator of M as an $R/\operatorname{Ann}(M)$-module is $\{0\}$.

(3) For any submodules U and V of M, we have

$$\operatorname{Ann}(U + V) = \operatorname{Ann}(U) \cap \operatorname{Ann}(V).$$

(4) For any submodules U and V of M, we have

$$(U : V) = \operatorname{Ann}((U + V)/U).$$

Definition. An R-module M is called **noetherian** if every ascending chain of submodules $M_0 \subset M_1 \subset M_2 \subset \dots$ stabilizes, i.e. there exists some $n \in \mathbb{N}$ such that $M_n = M_{n+k}$ for all $k \in \mathbb{N}$. A ring R is called **noetherian** if it is noetherian as an R-module.

3.1.12 Exercise. Show that a ring is noetherian if and only if every ideal is finitely generated. More generally, an R-module is noetherian if and only if it is finitely generated.

Definition. A **(homo-)morphism** $\varphi : M \to N$ of R-modules (sometimes also called R-**linear map**) is a map satisfying $\varphi(ax + by) = a\varphi(x) + b\varphi(y)$ for all $a, b \in R$ and $x, y \in M$. The **image** $\operatorname{im}(\varphi)$ of φ is the set $\{\varphi(x) \mid x \in M\}$. The **kernel** of φ is the set $\{x \in M \mid \varphi(x) = 0\}$.

3.1.13 Exercise. Both image and kernel of any homomorphism of R-modules are R-modules.

Definition. Let $I \subset \mathbb{Z}$ be an interval (meaning $I = [a, b] \cap \mathbb{Z}$ for some integers $a < b$). A **sequence** of R-modules is a family $(M_i)_{i \in I}$ of R-modules together with R-module homomorphisms $\varphi_i : M_{i-1} \to M_i$ for all $i \in I$ such that $i - 1 \in I$. The sequence is **exact at position** $i \in I$ (with $i - 1, i + 1 \in I$) if the image of φ_i and the kernel of φ_{i+1} are equal, i.e.

$$\operatorname{im}(\varphi_i) = \ker(\varphi_{i+1}) \subset M_i.$$

A sequence is **exact** if it is exact in every position. A **short exact sequence** is an exact sequence of the form

$$0 \to N \to M \to P \to 0.$$

3.1.14 Example. (1) The sequence $0 \to N \to M$ is exact at N if and only if the map $N \to M$ is injective.

(2) The sequence $M \to P \to 0$ is exact at P if and only if the map $M \to P$ is surjective.

(3) So the sequence $0 \to N \to M \to 0$ is exact at M if and only if the map $N \to M$ is an isomorphism.

3.1.15 Proposition. *Given a short exact sequence*

$$0 \to N \xrightarrow{\varphi} M \xrightarrow{\psi} P \to 0$$

of R-modules, we have that M is noetherian if and only if both N and P are noetherian.

Proof. If M is noetherian, then a direct argument shows that N and P are noetherian. Indeed, any ascending chain $N_0 \subset N_1 \subset \dots \subset N$ of submodules of N gives

the ascending chain $\varphi(N_0) \subset \varphi(N_1) \subset \ldots$ in M, which stabilizes by noetherianity of M. This implies that the original chain of submodules also stabilizes showing that N is noetherian. Any ascending chain $P_0 \subset P_1 \subset \ldots \subset P$ of submodules of P again gives the ascending chain $\psi^{-1}(P_0) \subset \psi^{-1}(P_1) \subset \ldots \subset M$ of submodules of M, which stabilizes. This shows again that the original chain also stabilizes and that P is noetherian.

Conversely, let $M_0 \subset M_1 \subset M_2 \subset \ldots$ be an ascending chain of submodules of M. Then we get ascending chains in both N and P, namely $\varphi^{-1}(M_0) \subset \varphi^{-1}(M_1) \subset \ldots \subset N$ and $\psi(M_0) \subset \psi(M_1) \subset \ldots \subset P$. By noetherianity of N and P, both chains eventually stabilize. So we can choose an $n \in \mathbb{N}$ such that for any $k > n$ we have $\varphi^{-1}(M_k) = \varphi^{-1}(M_n)$ and $\psi(M_k) = \psi(M_n)$. We show that this implies $M_k = M_n$ proving the claim. Pick $x \in M_k \supset M_n$. Then $\psi(x) \in \psi(M_k) = \psi(M_n)$ so that there exists a $y \in M_n$ with $\psi(x) = \psi(y)$. So the element $x - y \in M_k$ is in the kernel of ψ, which is the image of φ. So there is an element $z \in \varphi^{-1}(M_k) = \varphi^{-1}(M_n)$ with $\varphi(z) = x - y$. Finally,

$$x = (x - y) + y = \varphi(z) + y$$

shows that $x \in M_n$ and therefore $M_k = M_n$. ∎

3.1.16 Corollary. *Every submodule and every quotient module of a noetherian module is noetherian.*

Proof. Exercise: write the correct short exact sequence. ∎

3.1.17 Theorem (Hilbert's basis theorem). *The polynomial ring $R[t]$ over a noetherian ring R is noetherian. In particular, the polynomial ring $k[x_1, \ldots, x_n]$ over a field is noetherian.*

Proof. Let I be an ideal of $R[t]$ and set

$$J = \{\mathrm{LC}(f) \mid f \in I\}$$

where $\mathrm{LC}(f)$ is the leading coefficient of f. This set J is an ideal of R and therefore finitely generated by assumption, say $J = \langle a_1, \ldots, a_m \rangle$. For each $i \in [m]$ pick a polynomial $f_i \in I$ with $\mathrm{LC}(f_i) = a_i$ and set $I' = \langle f_1, \ldots, f_m \rangle \subset I$. Let d be the largest degree of the f_i.

We first show that any polynomial $f \in I$ of degree $k \geq d$ can be written as $f = g + h$ for a polynomial $h \in I'$ and a polynomial g of degree less than d. Write $f = \sum_{i=0}^{k} b_i t^i$. Then there are $u_j \in R$ such that $b_k = \sum_{j=1}^{m} u_j a_j \in J$. This identity implies that the polynomial

$$f - \sum_{j=1}^{m} u_j f_j t^{k-\deg(f_j)} \in I$$

has degree less than k. Iterating this process, we get a representation $f = g + h$ as claimed, i.e. $h \in I'$ and $\deg(g) < d$.

Set $M = R[t]_{<d}$ to be the R-submodule of $R[t]$ generated by the monomials

$1, t, \ldots, t^{d-1}$. The above argument shows that, as R-modules, we have

$$I = (I \cap M) + I'.$$

As a finitely generated module over a noetherian ring, the module M is noetherian by Corollary 3.1.16 so that $I \cap M$ is finitely generated (as an R-module). If $g_1, \ldots, g_n$ generate $I \cap M$, then I is finitely generated, namely

$$I = \langle f_1, \ldots, f_m, g_1, \ldots, g_n \rangle.$$

■

3.1.18 Corollary. *For any noetherian ring R and any $n \in \mathbb{N}$ the polynomial ring $R[x_1, \ldots, x_n]$ is noetherian. In particular, $S = k[x_1, \ldots, x_n]$ is noetherian for any field k.*

Proof. By induction on n, using Theorem 3.1.4 as the base case for the second sentence S. ■

Let us look at some notions from linear algebra in this more general contexts of R-modules. Note that finitely generated modules over fields are finite-dimensional vector spaces. So let R be a ring and M an R-module. Let $\mathcal{F} = (x_i)_{i \in I}$ be some family of elements $x_i \in M$. An R-**linear relation** in $\mathcal{F}$ is an identity

$$a_1 x_{i_1} + a_2 x_{i_2} + \ldots + a_k x_{i_k} = 0$$

for some $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in R$ and distinct elements $i_1, \ldots, i_k \in I$. An R-linear relation is called **non-trivial** if at least one coefficient a_j is not 0. The family $\mathcal{F}$ of elements of M is R-**linearly independent** if there is no non-trivial R-linear relation in $\mathcal{F}$.

Definition. Let M be an R-module M. A family $\mathcal{F} = (x_i)_{i \in I}$ of elements in M is called a **basis** of M if it is a linearly independent generating set. The module M is called **free** if it has a basis.

3.1.19 Example.
(1) Vector spaces over a field k are free k-modules (assuming Zorn's Lemma; otherwise, at least all finite-dimensional vector spaces are free k-modules).
(2) For every ring R and every $n \in \mathbb{N}$, the R-module R^n is a free R-module with basis $e_1, \ldots, e_n$.
(3) The $\mathbb{Z}$-module $\mathbb{Z}/m$ is not free for any $m \in \mathbb{Z}$, $m \neq 0$.

3.1.20 Exercise. Find a minimal generating set of $\mathbb{Z}$ as a $\mathbb{Z}$-module that is not a basis.

We will see free modules later in the context of Betti numbers. As far as R-module homomorphisms go, free modules behave much like vector spaces. In particular, the following result holds.

3.1.21 Theorem. *Let M be a free R-module with basis $(x_i)_{i \in I}$. Let N be an R-module and choose a family $(y_i)_{i \in I}$ of elements in N. There is a unique R-module homomorphism $\varphi \colon M \to N$ satisfying $\varphi(x_i) = y_i$ for all $i \in I$. If $(y_i)_{i \in I}$ is a basis of N, then φ is an isomorphism.*

Proof. Every $x \in M$ has a unique representation $x = \sum_{i\in I} a_i x_i$ as a (finite!) R-linear combination of the basis elements of M. Hence, we must have $\varphi(x) = \sum_{i\in I} a_i y_i$. This map is R-linear and hence uniquely determined by $\varphi(x_i) = y_i$.

If $(y_i)_{i\in I}$ is a basis of N, the inverse of φ is the map $\psi\colon N \to M$ determined by $\psi(y_i) = x_i$. ∎

3.1.22 Exercise. Let M be an R-module and $n \in \mathbb{N}$. Show that the following are equivalent.

(1) M can be generated by (at most) n elements.
(2) There is a surjective R-module homomorphism $R^n \to M$.
(3) M is isomorphic to a quotient module of R^n.

(For this exercise, we assume homomorphism and isomorphism theorems, as well as the quotient construction, that is not explicitly explained in these lecture notes.)

3.1.23 Exercise. Show that the module $\mathrm{Hom}_R(M, R)$ of R-module homomorphisms from M to R is free for every free R-module M.
Hint: dual basis

3.2. Prime ideals and localization

Next week

Chapter 4: Monomial ideals

4.1. Basic properties

Let k be a field and write $S = k[x_1, \ldots, x_n]$ for the polynomial ring over K (in n variables). The set

$$\mathrm{Mon}(S) = \{x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \mid \alpha \in \mathbb{Z}_{\geq 0}^n\}$$

of **monomials** in S is a basis of S as a k-vector space. For a polynomial

$$f = \sum_{u \in \mathrm{Mon}(S)} a_u \cdot u \in S$$

the set $\mathrm{supp}(f) = \{u \in \mathrm{Mon}(S) \mid a_u \neq 0\}$ is the **support** of f.

Definition. An ideal $I \subset S$ is a **monomial ideal** if I can be generated by monomials.

4.1.1 Exercise. What is the monomial ideal $\langle t^4, t^7 \rangle \subset k[t]$? It should be a principal ideal since $k[t]$ is a principal ideal domain.

4.1.2 Proposition. *Let $I \subset S$ be a monomial ideal. The set N of monomials contained in I is a k-basis of the vector space I.*

Proof. Exercise. ∎

This result has direct, nice consequences. First is an equivalent characterization of monomial ideals.

4.1.3 Corollary. *Let $I \subset S$ be an ideal. The following are equivalent.*

(1) I is a monomial ideal.

(2) For every polynomial $f \in S$ we have $f \in I$ if and only if $\mathrm{supp}(f) \subset I$. ∎

The second is about the quotient as a k-vector space.

4.1.4 Corollary. *Let $I \subset S$ be a monomial ideal. The residue classes of all monomials that are not contained in I form a basis of the k-vector space S/I.* ∎

The membership problem for monomials in monomial ideals given by a monomial generating sets is simple.

4.1.5 Proposition. *Let $\{u_1, \ldots, u_m\} \subset \mathrm{Mon}(S)$ be a monomial set of generators for a monomial ideal $I \subset S$. Then a monomial $v \in \mathrm{Mon}(S)$ is in I if and only if there exists a monomial $w \in \mathrm{Mon}(S)$ and an $i \in [m]$ such that $v = wu_i$.*

Proof. Exercise. ∎

This implies that a monomial ideal has a distinguished generating set.

4.1.6 Proposition. *Each monomial ideal of S has a unique minimal set of monomial generators. Concretely, let G be the set of monomials in I which are minimal with respect to divisibility. Then G is the unique minimal set of monomial generators for I.*

Proof. Exercise using the previous result on membership test. ∎

4.2. Algebraic operations

To recall some results from commutative algebra, we discuss standard algebraic operations of ideals in the special case of monomial ideals $I \subset S$. For a monomial ideal $I \subset S$, write $G(I)$ for the minimal monomial generating set in Proposition 4.1.6.

4.2.1 Exercise. Let $I, J \subset S$ be monomial ideals. Show that $G(I+J) \subset G(I \cup J)$ and $G(IJ) \subset G(I)G(J)$. Conclude that the sum as well as the product of monomial ideals are monomial ideals.

For two monomials $u, v \in \mathrm{Mon}(S)$, write $\gcd(u,v)$ for the greatest common divisor of u and v; write $\mathrm{lcm}(u,v)$ for the least common multiple of u and v.

4.2.2 Proposition. *Let $I, J \subset S$ be monomial ideals. The intersection $I \cap J$ is a monomial ideal generated by $\{\mathrm{lcm}(u,v) \mid u \in G(I), v \in G(J)\}$.*

Proof. For any $f \in I \cap J$, we have $\mathrm{supp}(f) \subset I \cap J$ by Corollary 4.1.3. This equivalence then also shows that $I \cap J$ is actually a monomial ideal.

Now let $w \in \mathrm{supp}(f)$ for $f \in I \cap J$ be a monomial occurring in f. Then there is a monomial $u \in G(I)$ dividing w and a monomial $v \in G(J)$ dividing w. This implies that $\mathrm{lcm}(u,v)$ divides w. ∎

4.2.3 Exercise. Is $G(I \cap J) = \{\mathrm{lcm}(u,v) \mid u \in G(I), v \in G(J)\}$ for monomial ideals $I, J \subset S$?

Definition. For ideals $I, J \subset S$, the **colon ideal** is defined as

$$I : J = \{f \in S \mid f \cdot J \subset I\}.$$

4.2.4 Proposition. *For two monomial ideals $I, J \subset S$, the colon ideal $I : J$ is also a monomial ideal. We have*

$$I : J = \bigcap_{v \in G(J)} I : \langle v \rangle$$

and $\{u/\gcd(u,v) \mid u \in G(I)\}$ is a monomial generating set of $I : \langle v \rangle$.

Proof. Again, we can show that $I : J$ is a monomial ideal by using Corollary 4.1.3. The essential point this time is that $\mathrm{supp}(f)v = \mathrm{supp}(fv) \subset I$ for any polynomial $f \in I$ and monomial $v \in G(J)$.

The presentation $I : J = \bigcap_{v \in G(J)} I : \langle v \rangle$ is direct. The monomial set of generators for $I : \langle v \rangle$ is an elementary argument about greatest common divisors. These are left as an exercise. ∎

Definition. Let $\mathfrak{m} = \langle x_1, \dots, x_n \rangle \subset S$ the homogeneous maximal ideal of S. The **saturation** of an ideal $I \subset S$ is

$$I \colon \mathfrak{m}^\infty = \bigcup_{k=1}^{\infty} I \colon \mathfrak{m}^k.$$

4.2.5 Exercise. Show that $I \colon \mathfrak{m}^\infty$ is a monomial ideal for every monomial ideal $I \subset S$.

Definition. The **radical** of an ideal $I \subset S$ is the ideal

$$\sqrt{I} = \{f \in S \mid f^k \in I \text{ for some } k \in \mathbb{N}\}.$$

4.2.6 Proposition. *The radial ideal of a monomial ideal is again a monomial ideal.*

Proof. We use induction and some basis convex geometry for the proof of this statement. Let $f \in \sqrt{I}$ be a polynomial such that $f^k \in I$. Let us list $\operatorname{supp}(f) = \{x^{\alpha_1}, \dots, x^{\alpha_r}\}$. After relabelling, we can assume that α_1 is a vertex of the convex hull of the set $\{\alpha_1, \dots, \alpha_r\} \subset \mathbb{R}^n$, which means that α_1 is not in the convex hull of $\alpha_2, \dots, \alpha_r$. Suppose we could write

$$(x^{\alpha_1})^k = (x^{\alpha_1})^{k_1} (x^{\alpha_2})^{k_2} \cdot \ldots \cdot (x^{\alpha_r})^{k_r}$$

with $k = k_1 + k_2 + \ldots + k_r$ and $k_1 < k$. This implies that α_1 is a convex combination of $\alpha_2, \dots, \alpha_r$, namely

$$\alpha_1 = \sum_{i=2}^{r} \frac{k_i}{k - k_1} \alpha_i \text{ with } \sum_{i=2}^{r} \frac{k_i}{k - k_1} = 1.$$

This is a contradiction to the choice of α_1 as a vertex of the convex hull of $\operatorname{supp}(f)$. What this means for f^k is that the monomial $x^{k\alpha_1}$ cannot cancel with other terms in f^k. Differently put, we have $x^{k\alpha_1} \in \operatorname{supp}(f^k) \subset I$. This shows, using Corollary 4.1.3, $x^{\alpha_1} \in \sqrt{I}$ and hence $f - a_{\alpha_1} x^{\alpha_1} \in \sqrt{I}$. So we can proceed by induction on the number of elements of $\operatorname{supp}(f)$ to show $\operatorname{supp}(f) \subset \sqrt{I}$. The claim then follows from Corollary 4.1.3. ∎

Definition. A monomial $x^\alpha \in \operatorname{Mon}(S)$ is called **squarefree** if $\alpha \in \{0, 1\}^n$. For $u = x^\alpha \in \operatorname{Mon}(S)$, we write

$$\sqrt{u} = \prod_{i \colon \alpha_i \neq 0} x_i.$$

4.2.7 Example. The notation $\sqrt{u}$ for a monomial has nothing to do with a square root. For instance, we have $\sqrt{x_1^3 x_2 x_5^7} = x_1 x_2 x_5$.

4.2.8 Proposition. *For a monomial ideal I, the set $\{\sqrt{u} \mid u \in G(I)\}$ is a generating set for the radical $\sqrt{I}$. In particular, a monomial ideal is radical if and only if it has a generating set of squarefree monomials.*

Proof. Exercise (using the previous result Proposition 4.2.6). ∎

Based on this characterization of monomial radical ideals, we use the following term.

Definition. A monomial ideal is called **squarefree** if it is radical.