Combinatorics

Lecture Notes
Universität Leipzig

Summer 2024

Rainer Sinn

Version of May 10, 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

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

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

$$(U\colon V) = \operatorname{Ann}\left((U+V)/U\right).$$

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** $\varphi\colon M \to N$ 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 $\varphi_i\colon M_{i-1} \to M_i$ 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

Localization is an important technique in ring theory generalizing the construction of the fraction field. We will see it here to show some basic results involving prime ideals.

Definition. An ideal I of a ring R is **prime** if $I \neq R$ and for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or $b \in I$.

3.2.1 Exercise. Show that a principal ideal $\langle a \rangle \subset R$ is prime if and only if the element a is prime. (Recall that an element $a \in R$ is prime if for all $b, c \in R$ such that a is a divisor of $b \cdot c$ it follows that a divides b or c.)

3.2.2 Exercise. An ideal I of R is prime if and only if the quotient ring R/I is a domain, i.e. it has no non-trivial zero divisors. (Recall, an element $a \in R$ is called a **zero divisor** if there exists a $b \neq 0$ such that $a \cdot b = 0$. The trivial zero divisor is 0.)

Definition. A set $S \subset R$ in a ring R is called **multiplicative** if $1 \in S$ and for all $s_1, s_2 \in S$ we also have $s_1 s_2 \in S$.

3.2.3 Example. If $P \subset R$ is a prime ideal, then $S = R \setminus P$ is multiplicative.

If R is a domain and $S \subset R$ is multiplicative with $0 \notin S$, then the set

$$R[S^{-1}] = \left\{ \frac{a}{s} \,\middle|\, s \in S \right\} \subset \mathrm{Quot}(R)$$

is a subring of the fraction field of R. In particular, the elements of S are invertible in $R[S^{-1}]$.

3.2.4 Example. (1) In $\mathbb{Z}$ the set S of all odd numbers is multiplicative. The ring $\mathbb{Z}[S^{-1}]$ is the subset of $\mathbb{Q}$ of all fractions that can be written with an odd denominator. Similarly, the set T of all even numbers is multiplicative. So the ring $\mathbb{Z}[T^{-1}]$ contains all fractions that can be written with an even denominator.

(2) In any ring R and any element $s \in R$, the set $S = \{1, s, s^2, s^3, \dots\}$ of all powers of s is a multiplicative set.

Definition. Let M be an R-module and $S \subset R$ a multiplicative set. On $M \times S$ we define the relation

$$(x_1, s_1) \sim (x_2, s_2) \qquad \Longleftrightarrow \qquad \exists t \in S\colon t(s_2 x_1 - s_1 x_2) = 0.$$

(The t in this definition is only relevant for rings that have nontrivial zero divisors.)

3.2.5 Proposition. *Let R be a ring and $S \subset R$ be a multiplicative set.*

(1) The relation $\sim$ is an equivalence relation. Writing $\frac{x}{s}$ (or x/s) for the equivalence class of (x, s) and $M[S^{-1}]$ for the set of these equivalence classes, we define

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st} \text{ and } a \cdot \frac{x}{t} = \frac{ax}{t}.$$

*This makes $M[S^{-1}]$ into an R-Modul, called the **localization** of M with respect to S.*

(2) The R-module $R[S^{-1}]$ with multiplication

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

*is a ring with unit $\frac{1}{1}$ and zero element $\frac{0}{1}$, called the **localization** of R with respect to S. For any R-module M, the R-module $M[S^{-1}]$ becomes a $R[S^{-1}]$-module via*

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}.$$

Proof. This is mostly direct. The main point is to show that addition (and scalar multiplication) are well-defined. For addition. suppose $\frac{x}{s} = \frac{x'}{s'} \in M[S^{-1}]$ so that $u(s'x - sx') = 0$ for some $u \in S$. For $\frac{y}{t} \in M[S^{-1}]$ we then have

$$\frac{tx' + s'y}{s't} = \frac{tux' + s'uy}{s'tu} = \frac{stux' + ss'uy}{ss'tu} = \frac{s'tux + ss'uy}{ss'tu} = \frac{tux + suy}{stu} = \frac{tx + sy}{st}.$$

Therefore, whenever we want to compute $\frac{x}{s} + \frac{y}{t}$, we can first find a common denominator and replace $\frac{x}{s}$ by $\frac{xt}{st}$ and $\frac{y}{t}$ by $\frac{ys}{st}$. Then associativity of addition in $M[S^{-1}]$ follows from associativity in M. To see that $M[S^{-1}]$ is still an abelian group, note

$$\frac{0}{1} + \frac{x}{s} = \frac{x}{s} \quad \text{und} \quad \frac{x}{s} + \frac{-x}{s} = \frac{0}{s} = \frac{0}{1}$$

for all $\frac{x}{s} \in M[S^{-1}]$. Associativity (and normalization) of scalar multiplication as well as the distributive laws follow in the same vein. The remaining details (and a proof of claim (2)) are left as an exercise. ■

Localization of an R-module M with respect to $S \subset R$ comes with an R-linear map

$$\lambda_S \colon M \to M[S^{-1}],\ x \mapsto \frac{x}{1}.$$

For $M = R$ the map $\lambda_S \colon R \to R[S^{-1}]$ is also a ring homomorphism. By construction, the elements of S become units in $R[S^{-1}]$. Indeed, we have

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}$$

in $R[S^{-1}]$.

In general, $\lambda_S(x) = 0/1$ for $x \in M$ if and only if there is a $t \in S$ with $tx = 0$. So λ_S is injective if and only if no element of S annihilates any element of $M \setminus \{0\}$. In particular, $\lambda_S \colon R \to R[S^{-1}]$ is injective if and only if S does not contain any zero divisors. We usually will not distinguish between a and $\frac{a}{1}$ not between s^{-1} and $\frac{1}{s}$ even if R is not a subring of $R[S^{-1}]$.

3.2.6 Exercise. What is $R[S^{-1}]$ if $0 \in S$?

3.2.7 Exercise. Show that a ring R is a domain if and only if the set $S = R \setminus \{0\}$ is multiplicative. In this case, $R[S^{-1}]$ is equal to $\mathrm{Quot}(R)$.

3.2.8 Lemma. *Let $S \subset R$ be a multiplicative set. For any ideal I of R, the set*

$$I[S^{-1}] = \left\{ \frac{a}{s} \mid a \in I, s \in S \right\}$$

is an ideal of $R[S^{-1}]$. Any ideal of $R[S^{-1}]$ is of this form for a suitable ideal I of R.

Proof. That $I[S^{-1}]$ is an ideal of R is direct from the fact that addition and multiplication of $R[S^{-1}]$ are well-defined. If $J \subset R[S^{-1}]$ is an ideal, then $I = \lambda_S^{-1}(J) \subset R$ is an ideal of R and we have $J = I[S^{-1}]$. ■

3.2.9 Theorem. *Let $P \subset R$ be a prime ideal and $S \subset R$ be a multiplicative set. If $P \cap S = \emptyset$, then the ideal $P[S^{-1}]$ is a prime ideal of $R[S^{-1}]$. Conversely, every prime ideal of $R[S^{-1}]$ is of the form $P[S^{-1}]$ of a prime ideal P of R with $P \cap S = \emptyset$.*

Let $S \subset R$ be multiplicative and $U \subset M$ be an R-submodule of an R-module M. We can argue directly that $U[S^{-1}]$ is a submodule of $M[S^{-1}]$. More generally, any R-linear map $\varphi \colon M \to N$ induces an $R[S^{-1}]$-linear map

$$\varphi_S \colon M[S^{-1}] \to N[S^{-1}],\ \frac{x}{s} \mapsto \frac{\varphi(x)}{s}.$$

We have $(\varphi \circ \psi)_S = \varphi_S \circ \psi_S$ and $(\mathrm{id}_M)_S = \mathrm{id}_{M[S^{-1}]}$. (Put differently, $M \mapsto M[S^{-1}]$ and $\varphi \mapsto \varphi_S$ gives a functor from the category of$R$-modules to the category of $R[S^{-1}]$-modules.) The next result is about properties of these assignments.

3.2.10 Theorem. *For any multiplicative set $S \subset R$ of a ring R localization is an exact functor. Concretely, this means that for all exact sequences*

$$\cdots \to M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \to \cdots$$

of R-modules the induced sequence

$$\cdots \to M_{i-1}[S^{-1}] \xrightarrow{\varphi_{i,S}} M_i[S^{-1}] \xrightarrow{\varphi_{i+1,S}} M_{i+1}[S^{-1}] \to \cdots$$

of $R[S^{-1}]$-modules is also exact.

Proof. We have to show $\operatorname{im}(\varphi_{i,S}) = \ker(\varphi_{i+1,S})$ for each position i. For $x/s \in M_{i-1}[S^{-1}]$ we have $\varphi_{i+1,S}(\varphi_{i,S}(x/s)) = \varphi_{i+1}(\varphi_i(x))/s = 0/s$. This shows the inclusion $\operatorname{im}(\varphi_{i,S}) \subset \ker(\varphi_{i+1,S})$. So let $y/s \in M_i[S^{-1}]$ such that $\varphi_{i+1,S}(y/s) = 0$. Then there is a $t \in S$ with $t\varphi_{i+1}(y) = 0$, so that $\varphi_{i+1}(ty) = 0$. Since we have $\ker(\varphi_{i+1}) = \operatorname{im}(\varphi_i)$ there is an $x \in M_{i-1}$ with $\varphi_i(x) = ty$. Then $y/s = ty/st = \varphi_i(x)/st = \varphi_{i,S}(x/st)$ showing the other inclusion $\ker(\varphi_{i+1,S}) \subset \operatorname{im}(\varphi_{i,S})$. ■

3.2.11 Exercise. Show that a sequence $\cdots \to M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \to \cdots$ is exact if and only if the sequences $0 \to \ker(\varphi_{i+1}) \to M_i \to \operatorname{im}(\varphi_{i+1}) \to 0$ are exact for all i (for which they make sense).

There are some useful, concrete consequences of this general statement. For instance, it implies that localization commutes with intersection or taking a quotient.

3.2.12 Corollary. *Let $S \subset R$ be a multiplicative set.*

(1) For any submodule U of any R-module M we have

$$(M/U)[S^{-1}] \cong M[S^{-1}]/U[S^{-1}].$$

(2) For any family $(U_i)_{i\in I}$ of submodules of any R-module M we have

$$\bigcap_{i\in I}\big(U_i[S^{-1}]\big) = \big(\bigcap\nolimits_{i\in I} U_i\big)[S^{-1}].$$

Proof. Exercise: find helpful exact sequences for the two claims. ■

We next look at ideals of the localization $R[S^{-1}]$ and their relation to ideals of R.

3.2.13 Proposition. *(1) For any ideal J in $R[S^{-1}]$ we have $J = \big(\lambda_S^{-1}(J)\big)[S^{-1}]$. The map $J \mapsto \lambda_S^{-1}(J)$ is an injection from the set of ideals in $R[S^{-1}]$ to the set of ideals in R.*

(2) The map $Q \mapsto \lambda_S^{-1}(Q)$ induces a bijection between the set of prime ideals in $R[S^{-1}]$ and the set of prime ideals P of R such that $P \cap S = \emptyset$. The inverse map is $P \mapsto P[S^{-1}]$. This bijection preservers inclusions and intersections.

Proof. Exercise. A useful fact is the statement that the preimage $\varphi^{-1}(Q)$ of any prime ideal $Q \subset S$ and any ring homomorphism $\varphi\colon R \to S$ is a prime ideal of R. (Why is that true?) Also, remember that the elements of $S \subset R$ become units in $R[S^{-1}]$ (for claim (2)). ■

Combining the previous two statements, we get the following special case (for R-modules U that are ideals of R).

3.2.14 Corollary. *Let $I \subset R$ be an ideal and S a multiplicative set. There is a canonical isomorphism*

$$(R/I)\left[\overline{S}^{-1}\right] \cong R[S^{-1}]/I[S^{-1}]$$

where we write $\overline{S} = \{s + I \mid s \in S\} \subset R/I$. ■

For any prime ideal P of R the set $R \setminus P$ is a multiplicative set. We use the short notation

$$R_P = R[(R \setminus P)^{-1}]$$

for the **localization of** R **with respect to** P. By the discussion above, the rings obtained in this way have the following special property (by Proposition 3.2.13).

Definition. A ring is called **local** if it has a unique maximal ideal.

In fact, Proposition 3.2.13 implies the following result.

3.2.15 Corollary. *For any prime ideal $P \subset R$ of R, the set of prime ideals of R_P is in bijection with the prime ideals of R that are contained in P. In particular, R_P is a local ring with maximal ideal PR_P.* ■

We record just two important observations about local rings (for now...).

3.2.16 Lemma. *Let R be a local ring with maximal ideal $\mathfrak{m}$. We have $R \setminus \mathfrak{m} = R^*$, which means that the units of R are exactly those elements that are not contained in the maximal ideal $\mathfrak{m}$.*

Proof. The proof is based on the simple observation that an element $a \in R$ is a unit if and only if $\langle a \rangle = R$ (and the fact that every proper ideal is contained in a maximal ideal by Zorn's Lemma). ■

For domains R (in particular polynomial rings over fields), the localizations R_P are naturally contained in the field $\mathrm{Quot}(R)$ (by Theorem 3.2.10). We can recover R from its localizations in the following sense.

3.2.17 Lemma. *Let R be a domain. For any prime ideal P of R the local ring R_P is a subring of* $\mathrm{Quot}(R)$ *and we have*

$$R = \bigcap_{\substack{\mathfrak{m} \subset R \\ \textit{maximales Ideal}}} R_{\mathfrak{m}}.$$

Proof. The inclusion $R \subset \bigcap R_{\mathfrak{m}}$ is direct by exactness of localization. For $x \in \mathrm{Quot}(R) \setminus R$ set $I = \{s \in R \mid sx \in R\}$. Then I is an ideal of R with $1 \notin I$. By Zorn's Lemma, I is contained in a maximal ideal $\mathfrak{m}$ of R. We must have $x \notin R_{\mathfrak{m}}$. Indeed, if $x = a/b$ in $\mathrm{Quot}(R)$ for $a, b \in R$, then $bx = a \in R$, which means $b \in I \subset \mathfrak{m}$. ■

3.3. Primary decomposition

Definition. An ideal I of R is called **primary** if $I \neq R$ and for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or there is a $k \in \mathbb{N}$ with $b^k \in I$.

3.3.1 Example. (1) Every prime ideal of every ring is primary.
(2) In $\mathbb{Z}$, the ideals $\langle p^k \rangle$ for any prime $p \in \mathbb{Z}$ and any $k \in \mathbb{N}$ are primary.

3.3.2 Exercise. (1) Show that an ideal I is primary if and only if for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or $b \in I$ or there is a $k \in \mathbb{N}$ such that both a^k and b^k are in I.
(2) Show that an ideal I is primary if and only if every zero divisor of R/I is nilpotent.

3.3.3 Exercise. If I is a primary ideal of R, then its radical ideal

$$\sqrt{I} = \{a \in R \mid \exists\, k \in \mathbb{N} \colon a^k \in I\}$$

is a prime ideal of R. (We usually say that I is P-primary for $P = \sqrt{I}$. e.g. $\langle p^k \rangle$ is $\langle p \rangle$-primary (or just p-primary) in $\mathbb{Z}$ for any $k \in \mathbb{N}$.)

3.3.4 Example. The converse of the claim in the above exercise is not true: if the radical of an ideal is prime, it does not need to be primary. Here is a standard example: Let $R = k[x, y, z]/\langle xy - z^2 \rangle$ for a field k and consider $P = \langle \overline{x}, \overline{z} \rangle \subset R$ and $I = \langle \overline{x}^2, \overline{xy}, \overline{xz} \rangle = P^2 \subset R$ so that $\sqrt{I} = P$ by construction. The point is that I is not primary. To see this, take $\overline{xy} = \overline{z}^2 \in I$; since $\overline{y}^k \notin I$ for any $k \in \mathbb{N}$ it follows that I is not primary. (A primary decomposition of I actually is $I = \langle \overline{x} \rangle \cap \langle \overline{x}^2, \overline{xz}, \overline{y} \rangle$.)

The example shows even more strongly that a power of a prime ideal does not need to be primary in general. (In $\mathbb{Z}$, for example, this statement is true.)

More generally, we consider primary ideals associated to R-modules in the following sense.

Definition. Let R be a ring and M be an R-module. We call a prime ideal $P \subset R$ **associated** to M (or an **associated prime ideal**) if there exists an element $x \in M$ such that $P = \operatorname{Ann}(x)$, that is

$$P = \{a \in R \mid ax = 0 \in M\}.$$

We write $\operatorname{Ass}(M)$ for the set of associated prime ideals.

A prime ideal $P \subset R$ is a **minimal prime ideal** of M if the module M_P is non-trivial and $M_Q = \{0\}$ for each prime ideal $Q \subset R$ properly contained in P.

3.3.5 Exercise. Let $I \subset R$ be an ideal. Show that a prime ideal $P \subset R$ is a minimal prime ideal of the R-module R/I if and only if $I \subset P$ and there is no prime ideal Q properly contained in P with $I \subset Q$.

If R is noetherian and M is finitely generated (as an R-module), then every minimal prime of M is actually an associated prime as well. This statement requires proof (see standard textbooks in commutative algebra, e.g. Matsumura's textbook). Here is a somewhat related statement.

3.3.6 Exercise. An ideal $I \subset R$ of a noetherian ring R is P-primary if and only if $\operatorname{Ass}(R/I) = \{P\}$. (We will often write $\operatorname{Ass}(I)$ instead of $\operatorname{Ass}(R/I)$.)

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

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

4.2.5 Exercise. Show that $I : \mathfrak{m}^\infty$ 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 $\operatorname{supp}(f) = \{x^{\alpha_1}, \ldots, x^{\alpha_r}\}$. After relabelling, we can assume that α_1 is a vertex of the convex hull of the set $\{\alpha_1, \ldots, \alpha_r\} \subset \mathbb{R}^n$, which means that α_1 is not in the convex hull of $\alpha_2, \ldots, \alpha_r$. 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 $\alpha_2, \ldots, \alpha_r$, 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.

4.3. Primary decomposition and associated primes

Here are some general facts from commutative algebra that we will now revisit for monomial ideals. Every ideal $I \subset S$ has a **primary decomposition**

$$I = \bigcap_{i=1}^{m} Q_i$$

for primary ideals $Q_i \subset S$. Such a decomposition is called **irredundant** (or **minimal**) if no ideal in the intersection on the right can be dropped. An ideal $Q \subset S$ is **primary** if for all $a, b \in S$ the condition $ab \in Q$ implies $a \in Q$ or $b \in \sqrt{Q}$. The following statements are correct and can be found in standard textbooks on commutative algebra (e.g. Atiyah, Macdonald): The radical of a primary ideal is prime. The prime ideals $P_i = \sqrt{Q_i}$ in an irredundant primary decomposition of I are unique. The primary ideals Q_i in a primary decomposition of I with the property that the corresponding prime ideal $P_i = \sqrt{Q_i}$ is minimal among these prime ideals are unique.

The following statement shows that every monomial ideal has a primary decomposition into monomial ideals, as we will see throughout this section.

4.3.1 Theorem. *Let $I \subset S$ be a monomial ideal. The ideal I is the intersection $I = \bigcap_{i=1}^{m} Q_i$ of ideals Q_i generated by powers of variables; so each Q_i is of the form $\langle x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k} \rangle$. There is one unique irredundant representation of this form.*

Proof. We first prove existence constructively. Let $G(I) = \{u_1, \dots, u_r\} \subset \mathrm{Mon}(S)$ be the minimal monomial generating set of I (see Proposition 4.1.6). If u_1 is not a power of a variable, then we can write $u_1 = v \cdot w$ for coprime monomials $v, w \in \mathrm{Mon}(S)$. For the ideal I we get $I = I_1 \cap I_2$ for $I_1 = \langle v, u_2, \dots, u_r \rangle$ and $I_2 = \langle w, u_2, \dots, u_r \rangle$ (Check!). This shows the existence of an irredundant representation $I = \bigcap_{i=1}^{m} Q_i$ as claimed.

To show uniqueness, suppose $\bigcap_{i=1}^{r} Q_i = \bigcap_{j=1}^{s} Q'_j$. It suffices to show for every $i \in [r]$ that there is some $j \in [s]$ with $Q'_j \subset Q_i$. By symmetry and the fact that both representations are irredundant, we get $r = s$ and $\{Q_1, \dots, Q_r\} = \{Q'_1, \dots, Q'_s\}$.

To simplify notation, fix $i \in [r]$ and assume $Q_i = \langle x_1^{a_1}, \dots, x_k^{a_k} \rangle$. If $Q'_j \not\subset Q_i$, there is a monomial $x_{\ell_j}^{b_j} \in Q'_j \setminus Q_i$. So we have $\ell_j \notin [k]$ or $b_j < a_j$. So in case that $Q'_j \not\subset Q_i$ for any $j \in [s]$, set

$$u = \mathrm{lcm}\{x_{\ell_1}^{b_1}, \dots, x_{\ell_s}^{b_s}\}.$$

This monomial is in $\bigcap_{j=1}^{s} Q'_j$ by construction and hence in Q_i. So $x_i^{a_i}$ divides u for some $i \in [r]$ which is a contradiction. ∎

Definition. We call a monomial ideal $I \subset S$ **irreducible** if it cannot be written as the intersection of two other monomial ideals. Otherwise, it is called **reducible**.

4.3.2 Exercise. Find examples for both reducible as well as irreducible monomial ideals.

Use Theorem 4.3.1 to show the following characterization of irreducible monomial ideals.

4.3.3 Corollary. *A monomial ideal is irreducible if and only if it can be generated by monomials that are all powers of variables.* ■

4.3.4 Example. Consider the monomial ideal

$$I = \langle x_1^2 x_2, x_1^2 x_3^2, x_2^2, x_2 x_3^2 \rangle \subset k[x_1, x_2, x_3].$$

Following the algorithm in the proof of Theorem 4.3.1, we get

$$\begin{aligned} I &= \langle x_1^2, x_1^2 x_3^2, x_2^2, x_2 x_3^2 \rangle \cap \langle x_2, x_1^2 x_3^2, x_2^2, x_2 x_3^2 \rangle = \langle x_1^2, x_2^2, x_2 x_3^2 \rangle \cap \langle x_2, x_1^2 x_3^2 \rangle \\ &= \big(\langle x_1^2, x_2^2, x_2 \rangle \cap \langle x_1^2, x_2^2, x_3^2 \rangle\big) \cap \big(\langle x_2, x_1^2 \rangle \cap \langle x_2, x_3^2 \rangle\big) \\ &= \langle x_1^2, x_2^2, x_3^2 \rangle \cap \langle x_1^2, x_2 \rangle \cap \langle x_2, x_3^2 \rangle \end{aligned}$$

4.3.5 Exercise. Use the algorithm in the proof of Theorem 4.3.1 to decompose the monomial ideal $I = \langle x_1 x_3, x_2 x_4, x_3 x_4, x_2 x_3 \rangle \subset k[x_1, x_2, x_3, x_4]$.

Following the algorithm in the proof of Theorem 4.3.1 for squarefree monomial ideals, we get the following statement.

4.3.6 Corollary. *A squarefree monomial ideal is the intersection of monomial prime ideals.* ■

Definition. A **minimal prime ideal** (or just **minimal prime**) of an ideal I in a ring R is a prime ideal P with $I \subset P$ such that there is no prime ideal Q satisfying $I \subset Q \subsetneq P$. We write $\mathrm{Min}(I)$ for the set of minimal primes of I.

4.3.7 Lemma. *If an ideal I has an irredundant presentation $I = P_1 \cap P_2 \cap \ldots \cap P_m$ for prime ideals P_i, then* $\mathrm{Min}(I) = \{P_1, P_2, \ldots, P_m\}$.

Proof. If P is a minimal prime of I, then $P_1 \cdot P_2 \cdot \ldots \cdot P_m \subset I \subset P$ implies that $P_i \subset P$ for some i. The minimality of P implies $P_i = P$ so that $P \in \mathrm{Min}(I)$.

To show that every P_i is indeed minimial, we use localization, which commutes with intersection. This means that

$$IR_{P_i} = (P_1 \cap \ldots \cap P_m)R_{P_i} = P_i R_{P_i}.$$

If P_i were not a minimal prime ideal, say $I \subset Q \subsetneq P_i$, then IR_{P_i} would be contained in QR_{P_i}, which would be a proper subset of $P_i R_{P_i}$, contradiction. ■

This gives us the primary decomposition of radical monomial ideals.

4.3.8 Corollary. *Every minimal prime of a squarefree monomial ideal $I \subset S$ is a monomial ideal so that I is the intersection of monomial prime ideals*

$$I = \bigcap_{P \in \mathrm{Min}(I)} P.$$

Proof. Combine the previous two results Corollary 4.3.6 and Lemma 4.3.7. ■

More generally, every monomial ideal has a primary decomposition into monomial ideals. We show this based on Theorem 4.3.1.

4.3.9 Proposition. *The irreducible ideal $\langle x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k} \rangle$ is primary with radical $\langle x_{i_1}, \dots, x_{i_k} \rangle$.*

Proof. Set $Q = \langle x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k} \rangle$ and $P = \langle x_{i_1}, \dots, x_{i_k} \rangle$. We have $Q \subset P$ and also $P^m \subset Q$ for $m = \sum_{i=1}^k a_i$. So P is the only minimal prime ideal of Q. This implies $\sqrt{Q} = P$. What is left is to show that Q is primary. If the product uv is in Q for two monomials $u, v \in \mathrm{Mon}(S)$, then $x_{i_j}^{a_j}$ divides uv for some $j \in [k]$. If $x_{i_j}^{a_j}$ divides u, then $u \in Q$. Otherwise, v must be divisible by x_{i_j} so that $v^k \in Q$ for some sufficiently large k. To check the definition more generally, suppose $f \cdot g \in Q$ for some polynomials $f, g \in Q$. Since Q is a monomial ideal, we have $u \cdot v \in Q$ for all $u \in \mathrm{supp}(f)$ and all $v \in \mathrm{supp}(g)$ with $uv \in \mathrm{supp}(fg)$. If $f \notin Q$, then we can assume that $u \notin Q$ for all $u \in \mathrm{supp}(f)$ (by replacing f by $f - \sum_{u \in \mathrm{supp}(f) \cap Q} a_u u$). Then recursion on the monomials in $\mathrm{supp}(g)$ shows that each monomial in $\mathrm{supp}(g)$ is divisible by one of the variables x_{i_j}, which implies that $g^k \in Q$ for some sufficiently large $k \in \mathbb{N}$. ■

Now we know that every monomial ideal is the intersection of irreducible monomial ideals by Theorem 4.3.1 and that irreducible monomial ideals are primary by Proposition 4.3.9. This shows primary decomposition of monomial ideals into monomial ideals.

4.3.10 Example. Following the algorithm in the proof of Theorem 4.3.1 for the monomial ideal

$$I = \langle x_1^3, x_2^3, x_1^2 x_3^2, x_1 x_2 x_3^2, x_2^2 x_3^2 \rangle \subset k[x_1, x_2, x_3]$$

we get the irredundant presentation as the intersection of irreducible monomial ideals $I = \langle x_1^3, x_2^3, x_3^2 \rangle \cap \langle x_1^2, x_2 \rangle \cap \langle x_1, x_2^2 \rangle$. The two ideals $\langle x_1^2, x_2 \rangle$ and $\langle x_1, x_2^2 \rangle$ have the same radical (so that $\mathrm{Ass}(\langle x_1^2, x_2 \rangle) = \{\langle x_1, x_2 \rangle\} = \mathrm{Ass}(\langle x_1, x_2^2 \rangle)$). The irredundant primary decomposition is therefore

$$I = \langle x_1^3, x_2^3, x_3^2 \rangle \cap \langle x_1^2, x_1 x_2, x_2^2 \rangle.$$

The primary decomposition obtained in this way, using the algorithm in the proof of Theorem 4.3.1 and then coarsening it to an irredundant primary decomposition, is unique and called the **standard primary decomposition**. It is in general not the only one.

4.3.11 Exercise. Find a monomial ideal with at least two primary decompositions. Determine the standard one and show that there is at least one more. (Recall that the primary ideals associated to minimal primes are always unique; the example needs embedded components for this to have a chance to work.)

Here are a few consequences for primary decompositions of monomial ideals.

4.3.12 Corollary. *The associated prime ideals of a monomial ideal are also monomial ideals.* ■

4.3.13 Corollary. *For any monomial ideal $I \subset S$ and any associated prime $P \in \operatorname{Ass}(I)$ there exists a monomial $u \in S$ such that $P = I : \langle u \rangle$.*

Proof. We use here that for every associated prime ideal $P \in \operatorname{Ass}(I)$ there exists an element $f \in S$ such that $P = I : \langle f \rangle$. That we can choose f to be a monomial now follows from the irreducibility of monomial prime ideals as follows. For each variable $x_i \in P$ we have $x_i f \in I$ because $P = I : \langle f \rangle$. Since I is a monomial ideal, this implies that $x_i u \in I$ for all $u \in \operatorname{supp}(f)$. In terms of colon ideals, this says

$$P = I : \langle f \rangle \subset \bigcap_{u \in \operatorname{supp}(f)} I : \langle u \rangle.$$

Conversely, for $g \in \bigcap_{u \in \operatorname{supp}(f)} I : \langle u \rangle$ we have $ug \in I$ for all $u \in \operatorname{supp}(f)$ and hence $fg \in I$ meaning $g \in I : \langle f \rangle = P$. Overall, we have $P = \bigcap_{u \in \operatorname{supp}(f)} I : \langle u \rangle$. Since P is an irreducible ideal, the claim follows. ■

4.4. Squarefree monomial ideals and simplicial complexes

Definition. A **simplicial complex** on the set $[n] = \{1, 2, \ldots, n\} \subset \mathbb{N}$ is a collection Δ of subset of $[n]$ such that for every $F \in \Delta$ and $F' \subset F$ we have $F' \in \Delta$. The ground set $[n]$ is called the **vertex set** of Δ. The elements $F \in \Delta$ are called the **faces** of the simplicial complex.

In some sources the additional property $\{i\} \in \Delta$ for all $i \in [n]$ is required for a simplicial complex. This property naturally holds for many classes of examples, especially geometric examples.

4.4.1 Example.
(1) A central class of examples are **triangulations** (in algebraic topology, for instance). A basic version is given by triangulations of a convex polytope (e.g. in the plane).
(2) From a graph $G = ([n], E)$ we can construct the **clique complex** of G. This is the simplicial complex Δ on $[n]$ with faces $F \subset [n]$ such that the induced graph $(F, E|_F)$ is a complete graph (aka clique).

(Draw pictures for these examples!)

Definition. The **dimension** (occasionally also rank) $\dim(F)$ of a face F of a simplicial complex Δ is the number $|F| - 1 \in \mathbb{N}_0$. The dimension $\dim(\Delta)$ of Δ is the largest dimension of any face of Δ. Faces of dimension 1 are called **edges** of

Δ; faces of dimension 0 are called **vertices**. A **facet** of Δ is an inclusion maximal element of $\Delta \subset 2^{[n]}$. We write $\mathcal{F}(\Delta)$ for the set of facets of Δ.

A simplicial complex is called **pure** if all facets have the same dimension (or equivalently the same number of elements).

A simplicial complex Δ on $[n]$ is uniquely determined by its facets. Given the facets $F_1, \dots, F_k$ of Δ we can directly reconstruct

$$\Delta = \{F \subset [n] \mid \exists\, j \in [k] \colon F \subset F_j\}.$$

More generally, given elements $G_1, \dots, G_m \in \Delta$, we write $\langle G_1, \dots, G_m \rangle$ for the simplicial complex of subset of the G_j, i.e.

$$\langle G_1, \dots, G_m \rangle = \{G \subset [n] \mid \exists\, j \in [m] \colon G \subset G_j\}.$$

Definition. A **non-face** of a simplicial complex on $[n]$ is a subset $F \subset [n]$ such that $F \notin \Delta$. We write $\mathcal{N}(\Delta)$ for the set of minimal non-faces (with respect to inclusion in $2^{[n]}$).

4.4.2 Example. For $\Delta \subset 2^{[5]}$ with $\mathcal{F}(\Delta) = \{\{1,2,4\},\{1,2,5\},\{2,3\},\{3,4\}\}$ we have $\dim(\Delta) = 2$ and $\mathcal{N}(\Delta) = \{\{1,3\},\{3,5\},\{4,5\},\{2,3,5\}\}$.

The primary combinatorial data that we are interested in here is the number faces organized by dimension.

Definition. Let Δ be a simplicial complex on $[n]$ of dimension d. We write $f_i(\Delta)$ for the number of i-dimensional faces of Δ. The f-**vector** of Δ is the sequence

$$f(\Delta) = (f_0(\Delta), f_1(\Delta), \dots, f_d(\Delta))\,.$$

We set $f_{-1} = 1$.

In algebraic topology, triangulations are used to give a definition of the **Euler characteristic** $\chi(X)$ of a topological space X. It is, by definition, the alternating sum of the entries of the f-vector.

4.4.3 Example. Let $\Delta = 2^{[n]}$ be the trivial simplicial complex. Topologically, this is the ball of dimension n, so it is homotopy equivalent to a point. The f-vector of Δ is given by $f_i(\Delta) = \binom{n}{i+1}$ for $i = 0, 1, \dots, n-1$. It follows that the Euler characteristic $\chi(\Delta)$ of Δ is 1 because

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

For the Euler characteristic of the sphere of dimension $n-2$, we take the simplicial complex Δ' on $[n]$ whose facets are the subsets with $n-1$ elements. In other words, $\mathcal{N}(\Delta') = \{[n]\}$. The Euler characteristic $\chi(\Delta')$ of Δ' can be determined the same way. Now, however, we have to distinguish whether n is even or odd

$$\chi(\Delta') = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

Definition. Let Δ be a simplicial complex on $[n]$ and let $S = k[x_1, \dots, x_n]$ be a polynomial ring in n variables over a field k. For each subset $F \subset [n]$ we write

$$x_F = \prod_{i \in F} x_i$$

for the monomial corresponding to the indicator function of F. We define the **Stanley-Reisner ideal** of Δ to be

$$I_\Delta = \langle x_F \mid f \in \mathcal{N}(\Delta) \rangle$$

the ideal generated by the monomials corresponding to the minimal non-faces of Δ. The **Stanley-Reisner ring** of Δ is the quotient S/I_Δ.

4.4.4 Exercise. Show the following statements. For every non-face F of Δ we have $x_F \in I_\Delta$. For every face F of Δ we have $x_F \notin I_\Delta$.

In fact we have the following result.

4.4.5 Proposition. *The monomials $u = x^\alpha \in \mathrm{Mon}(S)$ such that $\{i \in [n] \mid \alpha_i \neq 0\} \in \Delta$ are a basis of the K-vector space S/I_Δ.*

Proof. By Corollary 4.1.4 it suffices to show that $u = x^\alpha \notin I_\Delta$ if and only if $F_u = \{i \in [n] \mid \alpha_i \neq 0\} \in \Delta$. We show this by contraposition. So first, let $u = x^\alpha \in \mathrm{Mon}(S)$ be a monomial such that $F_u \notin \Delta$. Then we have $u \in I_\Delta$ because u is then divisible by a monomial x_F for a non-face F of Δ. Indeed, if $F_u \notin \Delta$ it contains a minimal non-face $F \in \mathcal{N}(\Delta)$; then u is a multiple of x_F. Conversely, if $u \in \mathrm{Mon}(S)$ is in I_Δ, then it is a multiple of a generator of I_Δ by Proposition 4.1.5. By definition, the generators of I_Δ are the monomials x_F for $F \in \mathcal{N}(\Delta)$ so that we have $u = v \cdot x_F$ for some minimal non-face $F \in \mathcal{N}(\Delta)$. This implies $F \subset F_u$ and therefore $F_u \notin \Delta$. ■

To wrap up this introductory section to monomial ideals, we collect some exercises to recall some important points.

4.4.6 Exercise.

(1) Let $I \subset S$ be a monomial ideal. Show that S/I is a finite-dimensional vector space if and only if for all $i \in [n]$ there is an $a_i \in \mathbb{N}$ with $x_i^{a_i} \in I$.

(2) Compute the dimension of the k-vector space S/I for $I = \langle x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n} \rangle$ as a function of the $a_i \in \mathbb{N}$.

(3) Write $P_F = \langle x_i \mid i \in F \rangle$ for any subset $F \subset [n]$. For any $d \in [n]$ find the minimal monomial generating set $G(I)$ for

$$I = \bigcap_{F \,:\, |F| = d} P_F.$$

(4) Fix an integer $d \in \mathbb{N}$ and let $I_d \subset S$ be the ideal generated by all monomials x^α with $\sum_{i=1}^n \alpha_i = d$ and $\alpha_i < d$ for all i. Find the radical $\sqrt{I_d}$ of I_d.

(5) Find the standard primary decomposition of the ideals $I_d \subset k[x_1, x_2, x_3]$ defined in the previous problem for $n = 3$.