

The aim of this section is largely to present the relevant definitions that will be required in order to understand the Hilbert series and the relation to supersymmetric theories. Complete proofs and derivations are beyond the scope of this appendix but can be found in [?].

## 0.1 Definitions

**Definition 1** ((Graded) Rings:). *A ring  $R$  is an abelian group with a multiplication operation  $(a, b) \mapsto ab$  and an identity element  $1$  satisfying*

- *Associativity:  $a(bc) = (ab)c$*
- *Identity:  $1a = a1 = a$*
- *Distributivity :  $(b + c)a = ba + ca$*

*for all  $a, b, c \in R$ .  $R$  is commutative if  $ab = ba$  and for the remainder of the text we will always take  $R$  to be commutative. A graded ring is a ring  $R$  together with a direct sum decomposition*

$$R = \bigoplus_{i=0}^{\infty} R_i \quad \text{such that } R_i R_j \subset R_{i+j} \text{ for all } i, j. \quad (1)$$

**Definition 2** (Invertible Elements). *An invertible element in a ring  $R$  is an element  $a \in R$  such that  $ab = 1$  with  $b = a^{-1} \in R$  unique.*

**Definition 3** (Fields). *A field  $\mathbb{K}$  is a ring in which every nonzero element  $a \in K$  is invertible. For example  $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .*

**Definition 4** (Polynomials). *A polynomial  $f$  in  $x_1, \dots, x_n$  with coefficients in  $\mathbb{K}$  is a finite linear combination of monomials of the form  $f = \sum_{\alpha} f_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}$ . The set of all such polynomials is denoted by  $\mathbb{K}[x_1, \dots, x_n]$ . In particular  $\mathbb{K}[x_1, \dots, x_n]$  forms a  $\mathbb{Z}^n$ -graded ring where the grading is provided by degree.*

**Definition 5** (Ideals). *An ideal in a ring  $R$  is an additive subgroup  $I \subset R$  such that  $ap \in I$  for all  $a \in R$  and  $p \in I$ . An ideal is said to be generated by a subset  $S \subset R$  if every element  $p \in I$  can be written as*

$$p = \sum_i a_i s_i \quad (2)$$

*for  $a_i \in R$  and  $s_i \in S$ . In particular, for  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$*

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i \mid h_1, \dots, h_s \in \mathbb{K}[x_1, \dots, x_n] \right\} \quad (3)$$

*is an ideal of  $\mathbb{K}[x_1, \dots, x_n]$  which we call the ideal generated by  $f_1, \dots, f_s$ .*

**Definition 6** (Radical Ideals). *An ideal  $I$  is radical if  $f^m \in I$  if for some  $m \in \mathbb{Z}^+$  implies  $f \in I$ .*

**Definition 7** (Radical of an Ideal). *The radical  $\sqrt{I}$  of an ideal  $I \in \mathbb{K}[x_1, \dots, x_n]$  is*

$$\sqrt{I} = \{f | f^m \in I \text{ for some } m \in \mathbb{Z}^+\}. \quad (4)$$

*It follows  $I \subset \sqrt{I}$  (since  $f \in I$  implies that  $f^1 \in I$ ). Moreover the radical of an ideal  $I$  is always a radical ideal.*

**Definition 8** ((Graded) Modules). *Let  $R$  be a ring, an  $R$ -module  $M$  is an abelian group with an action of  $R$ ,  $R \times M \rightarrow M$  satisfying*

- *Associativity:*  $a(bm) = (ab)m$
- *Identity:*  $1m = m1 = m$
- *Distributivity :*  $(b + c)m = bm + cm$ ,  $a(m + n) = am + an$

*for all  $a, b \in R$  and  $m, n \in M$ . Let  $R = \bigoplus_{i=0}^{\infty} R_i$  be a graded ring. Then a graded module over  $R$  is a module  $M$  with a decomposition*

$$M = \bigoplus_{i=-\infty}^{\infty} M_i \quad \text{such that } R_i M_j \subset M_{i+j} \text{ for all } i, j \quad (5)$$

**Definition 9** (Affine Spaces). *Let  $\mathbb{K}$  be a field and  $n \in \mathbb{Z}^+$ . The  $n$ -dimensional affine space over  $\mathbb{K}$  is*

$$\mathbb{K}^n = \{(a_1, \dots, a_n) | a_1, \dots, a_n \in \mathbb{K}\}. \quad (6)$$

**Definition 10** (Affine Varieties). *Let  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$  then the affine variety defined by  $f_1, \dots, f_s$  is*

$$\mathfrak{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in \mathbb{K}^n | f_i(a_1, \dots, a_n) = 0 \forall i \in \{1, \dots, s\}\} \subset \mathbb{K}^n \quad (7)$$

**Definition 11** (Irreducible Varieties). *An affine variety  $\mathbf{V} \subset \mathbb{K}^n$  is said to be irreducible if whenever  $\mathbf{V}$  is written in the form  $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$ , where  $\mathbf{V}_1$  and  $\mathbf{V}_2$  are affine varieties, then either  $\mathbf{V}_1 = \mathbf{V}$  or  $\mathbf{V}_2 = \mathbf{V}$ .*

## 0.2 Algebra-Geometry Correspondence

Given an affine variety  $\mathbf{V} \subset \mathbb{K}^n$  (this will play the role of the moduli space of supersymmetric vacua  $\mathbf{M}$  (??)). To this variety we can associate to it an ideal  $\mathfrak{I}(\mathbf{V}) \subset \mathbb{K}[x_1, \dots, x_n]$  (this will play the role of an operator algebra, such as chiral ring, etc) using the following map

$$\mathfrak{I}(\mathbf{V}) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \forall (a_1, \dots, a_n) \in \mathbf{V}\}, \quad (8)$$

Algebra	$\leftrightarrow$	Geometry
Radical ideal $I = \sqrt{I}$		Affine variety $\mathbf{V} = \mathfrak{V}(I)$
Addition of ideals $I + J$		Intersection of varieties $\mathfrak{V}(I) \cap \mathfrak{V}(J)$
Product of ideals $IJ$		Union of varieties $\mathfrak{V}(I) \cup \mathfrak{V}(J)$
Prime ideal $I$		Affine irreducible variety $\mathfrak{V}(I)$
Regular sequence		Complete intersection

Table 1: *Summary of the algebra-geometry correspondence.*

the proof that this indeed gives an ideal can be found in [?]. On the other hand, given an ideal  $I \subset \mathbb{K}[x_1, \dots, x_n]$  we can associate to it a variety  $\mathfrak{V}(I)$  (see Definition 10)

$$\mathfrak{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in \mathbb{K}^n \mid f_i(a_1, \dots, a_n) = 0 \forall i \in \{1, \dots, s\}\} \subset \mathbb{K}^n. \quad (9)$$

It can be shown that  $\mathfrak{V}(\mathfrak{I}(\mathbf{V})) = \mathbf{V}$ . We therefore have two maps which provide a correspondence and affine varieties. However, in general, this correspondence is not one to one. For example let us consider the family of distinct ideals  $\langle x^n \rangle$  (with  $n \in \mathbb{N}$ ) in  $\mathbb{C}[x]$ , then it's easy to see that to the map (9) associates to each of them the same variety, namely  $\mathfrak{V}(x^n) = \{0\}$ .

**Theorem 1** (The (Strong) Nullstellensatz). *Let  $\mathbb{K}$  be algebraically closed and let  $I \subset \mathbb{K}[x_1, \dots, x_n]$  be an ideal, then*

$$\mathfrak{I}(\mathfrak{V}(I)) = \sqrt{I}. \quad (10)$$

In particular, this theorem tells us that the maps (8)-(9) provide us a one to one correspondence between affine varieties and radical ideals. This dictionary can be extended reformulating in algebraic terms geometrical problems, see Table 1. A particular useful class of ideals is provided by the so called *prime ideals*

**Definition 12** (Prime Ideals). *An ideal  $I \subset \mathbb{K}[x_1, \dots, x_n]$  is a prime ideal if  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  and  $fg \in I$ , implies either  $f \in I$  or  $g \in I$ .*

It's easy to prove that every prime ideal is also a radical ideal, and that moreover there is a one-to-one correspondence between *irreducible varieties* and prime ideals via the maps (8) & (9)[?].

**Definition 13** (Noetherian Rings). *A ring  $R$  is called Noetherian if there is no infinite ascending sequence of left (or right) ideals. Therefore, given any chain of left (or right) ideals,*

$$I_1 \subseteq \dots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \dots, \quad (11)$$

*there exists an  $n$  such that*

$$I_n = I_{n+1} = \dots \quad (12)$$

When  $R$  is a *Noetherian ring*, using the *Lasker-Noether theorem*, we can always decompose an ideal of  $R$  as an irredundant intersection of a finite set  $\{J_i\}$  of primary ideals [?], this procedure is called *primary decomposition*. In particular we can take into account the ideal  $I$  and we get

$$I = \bigcap_i J_i . \quad (13)$$

We can then consider the different radical ideals  $\sqrt{J_i}$  associated to each of the primary ideals in (13). When the  $J_i$  are all prime ideals we have a one to one correspondence between affine irreducible complex varieties and the radical ideals  $\sqrt{J_i}$ . This implies that the corresponding complex variety, can be written as

$$\mathbf{F} = \bigcup_i \mathfrak{V}(\sqrt{J_i}) , \quad (14)$$

in this way the algebraic approach turns out to be very powerful since it provides a systematic way to decompose the F-flat moduli space  $\mathbf{F}$  of a theory into different irreducible branches. Remarkably we can also establish when the space  $\mathbf{F}$  is a complete intersection.

**Definition 14** (Regular Sequence). *A sequence of non-constant polynomials  $P_1, P_2, \dots, P_r$  is said to be regular if for all  $i = 1, \dots, r$ ,  $P_i$  is not a zero divisor modulo the partial ideal  $(P_1, \dots, P_{r-i})$ .*

Given an ideal generated by a regular sequence the following theorem holds [?]

**Theorem 2.** *Given the ring of polynomials  $R = \mathbb{C}[x_1, \dots, x_n]$  and the ideal  $I \subset R$  then the algebraic variety associated to the quotient ring  $R/I$  is a complete intersection if and only if  $I$  is generated by a regular sequence of homogeneous polynomials.*

Therefore if the ideal is generated by a *regular sequence* of polynomials then we can use letter counting for the computation of the corresponding Hilbert series. For application of the above theorem in a different context see [?], we also refer the interested reader to Appendix A of that paper for a more detailed discussion related to this issue.

### 0.3 Hilbert Series

We are now in a position to define the Hilbert function and Hilbert series.

**Definition 15.** *Hilbert function & Hilbert series Let  $M$  be a finitely generated graded module over  $\mathbb{K}[x_1, \dots, x_n]$  graded by degree  $\deg x_i = 1$  for all  $i = 1, \dots, n$ . The Hilbert function is defined to be*

$$HF_M(s) := \dim_{\mathbb{K}} M_s , \quad (15)$$

note that  $HF$  is finite in every degree. The Hilbert series is then defined in a formal power series as the generating function for the Hilbert function

$$HS(\tau; M) := \sum_{s=0}^{\infty} HF_M(s) \tau^s = \text{Tr}_M \tau^E \quad (16)$$

and here  $E : M_s \rightarrow \mathbb{Z}$  stands for the operator which computes the degree of an element  $y \in M_s$   $E(y) = s$ . If  $M$  is generated by  $d$  homogeneous elements of degrees  $E_1, \dots, E_d$  the Hilbert series takes the form

$$HS(\tau; M) = \frac{P(\tau)}{\prod_{i=1}^d (1 - \tau^{E_i})} \quad (17)$$

where  $P(\tau)$  is a polynomial in the formal parameter  $\tau$  with integer coefficients.

For example, let  $M = \mathbb{K}[x_1, \dots, x_n]$  be a polynomial ring with degrees  $E(x_i) = 1$ . The Hilbert series is simply

$$HS(\tau; M) = \frac{1}{(1 - \tau)^n}. \quad (18)$$

The Hilbert function is therefore

$$HF_M(s) = \frac{\prod_{i=0}^{s-1} (n + i)}{s!}. \quad (19)$$

The results (16) & (17) may also be generalised to the case of rings with  $\mathbb{Z}^b$  grading  $M = \bigoplus_{s_1, s_2, \dots, s_b} M_{s_1 s_2 \dots s_b}$  in which case the result takes the general form

$$HS(\tau_1, \tau_2, \dots, \tau_b; M) = \text{Tr}_M \prod_{l=1}^b \tau_l^{E^{(l)}} = \frac{P(\tau_1, \dots, \tau_b)}{\prod_{i=1}^d \left( 1 - \prod_{l=1}^b \tau_l^{E_i^{(l)}} \right)}. \quad (20)$$

If we let  $\mathbf{M} = \mathfrak{V}(I)$  be the algebraic variety defined as the set of zeros of the ideal  $I \subset \mathbb{K}[x_1, \dots, x_n]$  then the Hilbert series of  $R = \mathbb{K}[x_1, \dots, x_n]/I$  (as written in the form (17)) allows us to compute the dimension of  $\mathbf{M}$  and the degree of  $\mathbf{M}$  (the number of intersection points of  $\mathbf{M}$  with  $d = \dim_{\mathbb{K}} \mathbf{M}$  generic hyperplanes)  $\deg \mathbf{M}$  as

$$\dim_{\mathbb{K}} \mathbf{M} = \dim_{\mathbb{K}} M = \text{Order of pole at } \tau = 1 \text{ of } HS(\tau; M) = d, \quad (21)$$

$$\deg \mathbf{M} = P(1). \quad (22)$$

## 0.4 Example Computations with *Macaulay2*

Let us present some example code for *Macaulay2* [?]. We firstly focus on the computations of the Hilbert series performed in the introduction ??.

Note that *Macaulay2* represents elements of  $\mathbb{C}$  via floating point approximations.  $\mathbb{C}$  is an example of an *inexact field*. *Macaulay2* uses Gröbner bases and the algorithms it uses do not work over  $\mathbb{C}$ . Therefore when performing practical computations we must instead work over  $\mathbb{Q}$  (or any other field of characteristic zero will do) while using *Macaulay2* before tensoring any final result with  $\mathbb{C}$ . Tensoring with  $\mathbb{C}$  can destroy some properties which may hold over  $\mathbb{Q}$ . For example an ideal that is prime over  $\mathbb{Q}$  may fail to be prime after tensoring with  $\mathbb{C}$ .<sup>1</sup> Hence the *Macaulay2* output should always be read with the above caveat in mind; nevertheless, our main object of interest, the Hilbert series is expected to be independent of the above.

The first example that we presented there was the most simple case of  $\mathcal{N} = 4$  SYM with gauge group  $G = U(1)$  (free theory). This computation can of course simply be performed by hand. Nevertheless one can also use *Macaulay2* by inputting  $F = R/I$  with  $R = \mathbb{C}[X, Y, Z]$  and  $I$  trivial.

```
i1 : R=QQ[X,Y,Z,Degrees=>{{1,0,0,0},{0,1,0,0},{0,0,1,0}}]
i2 : hilbertSeries(R)
```

This of course outputs the Hilbert series

$$o2 = \frac{1}{(1-T)^2(1-T)(1-T)^0}$$

One then takes the output and sets  $\tau_{1,2,3} = T_{0,1,2}$ .

For the second case presented in the introduction of the  $\mathcal{N} = 1$   $G = U(1)$  gauge theory with  $F = R/I$ ,  $R = \mathbb{C}[X, Y, Z]$  and  $I = \langle XY, XZ, YZ \rangle$  an example *Macaulay2* input is

```
i1 : R=QQ[X,Y,Z,Degrees=>{{1,0,0,1},{0,1,0,-1},{0,0,1,0}}]
i2 : I=ideal(X*Y,X*Z,Y*Z)
i3 : hilbertSeries(R/I)
i4 : primaryDecomposition I
i5 : radical I
i6 : isPrime I
```

This outputs

---

<sup>1</sup>See e.g. [?].

$$o3 = \frac{\begin{array}{ccccccc} & & & & -1 & & \\ & & & & & & \\ 1 & - & T & T & - & T & T & T & - & T & T & T & + & 2T & T & T \\ & 0 & 1 & & 0 & 2 & 3 & & 1 & 2 & 3 & & 0 & 1 & 2 \end{array}}{\begin{array}{ccccccc} & & & & -1 & & \\ & & & & & & \\ (1 & - & T & ) & (1 & - & T & T & ) & (1 & - & T & T & ) \\ & 2 & & & 1 & 3 & & & 0 & 3 \end{array}}$$

o4 = {ideal (X, Y), ideal (X, Z), ideal (Y, Z)}

o5 = monomialIdeal (X\*Y, X\*Z, Y\*Z)

o6 = false

Setting  $\tau_{1,2,3} = T_{0,1,2}$  and  $z = T_3$  identifies  $o3$  with (??).

We can also compute for more complicated non-abelian cases. Of course the computations become more and more complex with  $\dim G$ . Let us take the case of  $\mathcal{N} = 4$  SYM with gauge group  $G = SU(2)$ . In this case  $F = R/I$  with  $R = \mathbb{C}[X, Y, Z]$  where now  $X, Y, Z \in \mathfrak{su}(2)$

$$X = \begin{pmatrix} X_1 & X_2 \\ X_3 & -X_1 \end{pmatrix}, \quad Y = \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & -Y_1 \end{pmatrix}, \quad Z = \begin{pmatrix} Z_1 & Z_2 \\ Z_3 & -Z_1 \end{pmatrix} \quad (23)$$

The ideal is  $I = \langle [X, Y], [X, Z], [Y, Z] \rangle$  coming from the superpotential  $\text{tr } X[Y, Z]$ . We input

```
i1 : R=QQ[X1, X2, X3, Y1, Y2, Y3, Z1, Z2, Z3,
Degrees=>{{1, 0, 0, 0}, {1, 0, 0, -2}, {1, 0, 0, 2},
{0, 1, 0, 0}, {0, 1, 0, -2}, {0, 1, 0, 2},
{0, 0, 1, 0}, {0, 0, 1, -2}, {0, 0, 1, 2}}]

i2 : I=ideal(-*Y3*Z2 + *Y2*Z3, *Y3*Z1 - *Y1*Z3, -*Y2*Z1 + *Y1*Z2,
*X3*Z2 -*X2*Z3, -*X3*Z1 + *X1*Z3, *X2*Z1 - *X1*Z2,
-*X3*Y2 + *X2*Y3, *X3*Y1 - *X1*Y3, -*X2*Y1 + *X1*Y2)

i3 : hilbertSeries(R/I)

i4 : primaryDecomposition I

i5 : radical I

i6 : isPrime I
```

This outputs (here we have suppressed the output for the Hilbert series  $o3$  in the raw form to save on space, we present it in the simple form below)

```
o4 = {ideal (Y3*Z2 - Y2*Z3, X3*Z2 - X2*Z3, Y3*Z1 - Y1*Z3,
Y2*Z1 - Y1*Z2, X3*Z1 - X1*Z3, X2*Z1 - X1*Z2, X3*Y2 - X2*Y3,
X3*Y1 - X1*Y3, X2*Y1 - X1*Y2)}
```

```
o5 = ideal (Y3*Z2 - Y2*Z3, X3*Z2 - X2*Z3, Y3*Z1 - Y1*Z3,
Y2*Z1 - Y1*Z2, X3*Z1 - X1*Z3, X2*Z1 - X1*Z2, X3*Y2 - X2*Y3,
X3*Y1 - X1*Y3, X2*Y1 - X1*Y2)
```

```
o6 = true
```

After converting the raw output for the Hilbert series as before we have

$$\begin{aligned}
\text{HS}(\tau_1, \tau_2, \tau_3, z; F) = \text{PE}[\chi_2(z)(\tau_1 + \tau_2 + \tau_3)] & \left\{ 1 + \tau_1^2 \tau_2^2 \tau_3^2 \right. \\
& + (\chi_4(z) + \chi_2(z))\tau_1 \tau_2 \tau_3 + (\tau_1 + \tau_2)(\tau_1 + \tau_3)(\tau_2 + \tau_3) \\
& \left. - (\tau_1 \tau_2 + \tau_1 \tau_3 + \tau_2 \tau_3)\chi_2(z) - \chi_2(z)(\tau_1 + \tau_2 + \tau_3)\tau_1 \tau_2 \tau_3 \right\}
\end{aligned} \tag{24}$$