LECTURES ON REFLECTION GROUPS AND INVARIANT THEORY TAUGHT IN SS 2020 IN JENA

ANDRIY REGETA

To prepeare this course I used the material from the literature in References.

1. LECTURE 1 (Introduction to Invariant Theory).

The notion of an invariant is one of the most general concepts of mathematics. Whenever a group G acts on a set S we look for elements $s \in S$ which do not change under the action, i.e., which satisfy $g \cdot s = s$ for any $g \in G$. Let us introduce the formal definition of a group action.

Definition 1. Let G be a group and let S be a set. An action of G on S is a map $\cdot \colon G \times S \to S$ such that $1 \cdot s = s$ and $(gh) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$ and $s \in S$.

The set of all elements s in S which satisfy $g \cdot s = s$ for any $g \in G$ we denote by S^G. Of course, if a group G acts trivially on S, then $S^G = S$.

Let us consider now one of the most basic non-trivial examples.

Example 1. Let the group

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

be the subgroup of the group of invertable 2×2 matrices $\mathrm{GL}(2, \mathbb{C})$ over the field of complex numbers. Consider the two-dimensional vector space

$$W = \mathbb{C}w_1 \oplus \mathbb{C}w_2$$

generated by two linearly independent vectors w_1 and w_2. Assume also that $g \in G$ acts on W by matrix multiplication, i.e., $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ acts trivially on W and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ maps $aw_1 + bw_2$ to $bw_1 + aw_2$. Then it is easy to calculate that W^G is the one-dimensional vector space $\mathbb{C}(w_1 + w_2)$ generated by $w_1 + w_2$.

Roughly speaking, in this course we consider S to be a ring of polynomials endowed with a certain action of G and study the set of invariant polynomials. In this introductory lecture we introduce the notion of polynomial functions on a G-module W and the notion of invariants. Further, we consider some basic examples of invariants of some groups.

During the whole course **our basic field** is the **field of complex numbers** $\mathbb{C}$.

In the rest of Lecture 1 I closely follow [KrP14].

1.1. **Polynomial functions.** Let W be a finite dimensional $\mathbb{C}$-vector space. A function $f\colon W \to \mathbb{C}$ is called **polynomial** if it is given by a polynomial in the coordinates with respect to a basis of W. It is easy to see that this is independent of the choice of a coordinate system of W. We denote by $\mathbb{C}[W]$ the $\mathbb{C}$-algebra of polynomial functions on W which is usually called the **coordinate ring** of W or the **ring of regular functions** on W. If $w_1, \dots, w_n$ is a basis of W and $x_1, \dots, x_n$ the dual basis of the dual vector space W^* of W, i.e., the **coordinate functions**, we have $\mathbb{C}[W] = \mathbb{C}[x_1, \dots, x_n]$. This is a polynomial ring in the x_i.

A regular function $f \in \mathbb{C}[W]$ is called **homogeneous of degree** d if $f(tw) = t^d f(w)$ for all $t \in \mathbb{C}, w \in W$. Thus, $\mathbb{C}[W] = \oplus_d \mathbb{C}[W]_d$ is a graded $\mathbb{C}$-algebra, where $\mathbb{C}[W]_d$ denotes the subspace of homogeneous polynomials of degree d. (Recall that an algebra $A = \oplus_I A_i$ is **graded** if the multiplication satisfies $A_i A_j \subset A_{i+j}$). Choosing coordinates as above we see that the monomials $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ such that $d_1 + d_2 + \dots + d_n = d$ form a basis of $\mathbb{C}[W]_d$. Note that $\mathbb{C}[W]_1 = W^*$.

1.2. **Invariants.** As usual, we denote by $\mathrm{GL}(W)$ the **general linear group**, i.e., the group of non-degenerate linear maps from W to W. Choosing a basis $w_1, w_2, \dots, w_n$ of W we can identify $\mathrm{GL}(W)$ with the group $\mathrm{GL}_n(\mathbb{C})$ of invertible $n \times n$ matrices with entries in $\mathbb{C}$ in the usual way: the i-th column of the matrix A corresponding to the automorphism $g \in \mathrm{GL}(W)$ is the coordinate vector of $g(w_i)$ with respect to the chosen basis. Now assume that there is given a subgroup $G \subset \mathrm{GL}(W)$ or, more generally, a group G together with a **linear representation** on W, i.e., a group homomorphism

$$\rho\colon G \to \mathrm{GL}(W).$$

Note that in this course all our representations are going to be linear and instead of "linear representation" we will just use "representation".

The homomorphism ρ induces the **linear action** (in the future just **action**) of G on W as follows: $g \cdot w := \rho(g)w$ $(g \in G, w \in W)$, and we will call W a G-**module**.

Recall that the dual vector space to W is defined by

$$W^* = \{f\colon W \to \mathbb{C} \mid f(v + \alpha w) = f(v) + \alpha f(w)\},$$

where $v, w \in W$ and $\alpha \in \mathbb{C}$. If $\rho\colon G \to \mathrm{GL}(W)$ is a representation, then the dual representation $\rho^*\colon G \to \mathrm{GL}(W^*)$ is defined by

$$\rho^*(g)(f)(v) = f(\rho(g^{-1})v). \tag{1}$$

Remark 1. Let us check that this defines indeed a representation, i.e.,

$$(\rho^*(gh)(f))(v) = f(\rho((gh)^{-1})v) = f(\rho(h^{-1})\rho(g^{-1})v) = \rho^*(g)(f \circ \rho(h^{-1}))(v) = \rho^*(g)(\rho^*(h)(f))(v).$$

Now we define the action of G on $\mathbb{C}[W]$ as follows: if $x_1, \dots, x_n$ is a basis of W^*, then for each $g \in G$, $g \cdot x_i \in W^*$ is defined by (1), i.e., $g \cdot x_i(v) = \rho^*(g)(x_i)(v) = x_i(\rho(g^{-1})v)$, where $i = 1, \dots, n$. Further, let $f(x_1, \dots, x_n) \in \mathbb{C}[W]$, then

$$g \cdot f(x_1, \dots, x_n) = f(g \cdot x_1, \dots, g \cdot x_n) = f(\rho^*(g)(x_1), \dots, \rho^*(g)(x_n)).$$

Definition 2. A function $f \in \mathbb{C}[W]$ is called G-**invariant** or shortly **invariant** if $f(gw) = f(w)$ for all $g \in G$ and $w \in W$. The invariants form a subalgebra of $\mathbb{C}[W]$ called **invariant ring** and denoted by $\mathbb{C}[W]^G$.

Recall that the orbit of $w \in W$ is defined to be the subset $Gw := \{gw \mid g \in G\} \subset W$ and the **stabilizer** of w it the subgroup $G_w := \{g \in G \mid gw = w\}$. It is clear that a function is G-invariant if and only if it is constant on all orbits of G in W. A subset $X \subset W$ is called G-**stable** if it is a union of orbits, i.e., if one has $gx \in X$ for all $x \in X, g \in G$.

1.3. **Orbit space.**

Definition 3. Let G acts on a set S. We define an equivalence relation in the following way:

$$x \sim y \text{ if and only if } y = gx \text{ (and } x = g^{-1}y) \text{ for some } g \in G.$$

We call $S/\sim$ the **orbit space** which we denote by S/G.

Suppose G is a finite group that acts linearly on a vector space W, i.e., $G \subset \mathrm{GL}(W)$. Then one can show that the orbit space W/G has a natural structure of an affine variety (which we will define later on in this course). Moreover, as th polynomial ring $\mathbb{C}[W]$ can be treated as the "ring of functions" of W, $\mathbb{C}[W]^G$ is the ring of functions of the orbit space W/G. **So, the invariants are the functions on the orbit space.**

1.4. **Examples.** Let us consider now the classical example of quadratic forms.

Example 2. Consider the 3-dimensional vector space of quadratic forms

$$W = \{q(x, y) = a_0x^2 + a_1xy + a_2y^2 \mid a_0, a_1, a_2 \in \mathbb{C}\}.$$

Define an action of $\mathrm{SL}(2, \mathbb{C})$ on W by

$$\sigma \cdot q(x, y) := q(\alpha x + \gamma y, \beta x + \delta y),\ \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{C})$$

Let t_i be the linear map from W to $\mathbb{C}$ that maps a polynomial $a_0x^2 + a_1xy + a_2y^2$ to the coefficient a_i. The functions t_0, t_1 and t_2 form a basis of the dual space W^*. Hence, the coordinate ring $\mathbb{C}[W]$ can be identified with the ring of polynomials $\mathbb{C}[t_0, t_1, t_2]$.

One can prove that $\mathbb{C}[W]^{\mathrm{SL}_2} = \mathbb{C}[t_1^2 - 4t_0t_2]$. The term $t_1^2 - 4t_0t_2$ may be recognized as the discriminant of a quadratic equation.

Example 3. Let $\xi = e^{2\pi i/n}$ be a complex primitive n-th root of unity and let $\mu_n = \langle\xi\rangle \subset \mathbb{C}^*$ be the cyclic group of order n.

Let $g_\xi \colon \mathbb{C}^2 \to \mathbb{C}^2$ be given by the map

$$g_\xi(a, b) = (\xi a, \xi^{-1}b),$$

where $(a, b) \in \mathbb{C}^2$. Then $S = \mathbb{C}[x, y]$, where

$$x(a, b) = a, \quad y(a, b) = b$$

are the coordinate functions. So

$$(g_\xi x)(a, b) = x(\xi^{-1}a, \xi b) = \xi^{-1}a = \xi^{-1}x(a, b) \text{ so } g_\xi x = \xi^{-1}x, \text{ and}$$

$$(g_\xi y)(a, b) = y(\xi^{-1}a, \xi b) = \xi b = \xi^{-1}y(a, b) \text{ so } g_\xi y = \xi y.$$

Then xy, x^n, y^n are invariant under our action. We claim that any $f(x,y) \in S^G$, i.e., any polynomial invariant under our action, is a polynomial in xy, x^n, y^n. Indeed, let $f(x,y) = \sum_i a_{i,j} x^i y^j$, then

$$g_\xi f(x,y) = \sum_{i,j} a_{i,j} (\xi x)^i (\xi^{-1} y)^j = \sum_{i,j} a_{i,j} \xi^{i-j} x^i y^j = f = \sum_{i,j} a_{i,j} x^i y^j.$$

Since $\{x^r y^k \mid r, k \in \mathbb{N} \cup \{0\}\}$ form a basis of $\mathbb{C}[x,y]$ we have that $\xi^{i-j} = 1$ (whenever $a_{i,j} \neq 0$) which implies that n divides $|i-j|$. Hence, the summund

$$a_{i,j} x^i y^j = \begin{cases} a_{i,j} (xy)^i y^{j-i} & \text{if } i < j \\ a_{i,j} (xy)^j x^{i-j} & \text{if } j < i. \end{cases}$$

of f belongs to $\mathbb{C}[x^n, xy, y^n]$. Therefore, $f(x,y) \in \mathbb{C}[x^n, xy, y^n]$ and then $S^G = \mathbb{C}[x^n, xy, y^n]$.

2. LECTURE 2 (More examples and Noether's Theorem).

In this lecture we compute the ring of invariants for the multiplicative group of the field and for a symmetric group and list a few important results in the invariant theory of finite groups.

2.1. More example.

Example 4. We start with the two-dimensional representation of the multiplicative group $\mathbb{C}^* := \mathrm{GL}_1(\mathbb{C})$ on $W = \mathbb{C}^2$ given by

$$t \mapsto \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}.$$

Then the invariant ring is generated by xy: $\mathbb{C}[W]^{\mathbb{C}^*} = \mathbb{C}[xy]$. Indeed, let $f(x,y) = \sum_i a_{i,j} x^i y^j$ be the polynomial invariant ander action of $\mathbb{C}^*$, i.e.,

$$\sum_{i,j} a_{i,j} x^i y^j = \sum_i a_{i,j} (tx)^i (t^{-1} y)^j = \sum_i a_{i,j} t^{i-j} x^i y^j.$$

Since $\{x^r y^k \mid r, k \in \mathbb{N} \cup \{0\}\}$ form a basis of $\mathbb{C}[x,y]$ we have that $t^{i-j} = 1$ whenever $a_{i,j} \neq 0$. Since this should hold for any $t \in \mathbb{C}^*$, we get that $i - j = 0$.

Note that if we change the two-dimensional representation of the multiplicative group $\mathbb{C}^* := \mathrm{GL}_1(\mathbb{C})$ on $W = \mathbb{C}^2$ to the following one

$$t \mapsto \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}.$$

Then one can show that the invariant ring is trivial, i.e., $\mathbb{C}[V]^{\mathbb{C}^*} = \mathbb{C}$.
So, the invariant ring depends dramatically on the action of the group.

The next example is classical and deals with invariants of a symmetric group.

Example 5. Let S_n denote the **symmetric group** on $\{1, \dots, n\}$ and consider the natural representation of S_n on $V = \mathbb{C}^n$ given by $\sigma \cdot e_i = e_{\sigma(i)}$, or, equivalently

$$\sigma \cdot (x_1, x_2, \dots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

As above, S_n acts on the polynomial ring $\mathbb{C}[x_1, x_2, \dots, x_n]$ and the invariant functions are the **symmetric polynomials**:

$$\mathbb{C}[x_1, \dots, x_n]^{S_n} = \{f \mid f(x_{\sigma(1)}, \dots) = f(x_1, ...) \text{ for all } \sigma \in S_n\}.$$

It is well known and classical that every symmetric polynomial can be expressed uniquely as a polynomial in the elementary symmetric functions $h_1, h_2, \dots, h_n$ defined by

$$\begin{aligned} h_1 &:= x_1 + x_2 + \cdots + x_n, \\ h_2 &:= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\cdots \\ h_k &:= \sum_{i_1<i_2<\cdots<i_k} x_{i_1}x_{i_2}\dots x_{i_k} \\ &\cdots \\ h_n &:= x_1x_2\dots x_n. \end{aligned}$$

We will give a proof of this below.

Proposition 1. *The elementary symmetric functions $h_1, h_2, \dots, h_n$ are algebraically independent and generate the algebra of symmetric functions: $\mathbb{C}[x_1, x_2, \dots, x_n]^{S_n} = \mathbb{C}[h_1, h_2, \dots, h_n]$*

Proof. We proof this by induction on n. Let $h'_1, h'_2, \dots, h'_{n-1}$ denote the elementary symmetric functions in the variables $x_1, x_2, \dots, x_{n-1}$. Then

$$\begin{aligned} h_1 &= h'_1 + x_n, \\ h_2 &= h'_2 + x_nh'_1, \\ &\cdots \\ h_{n-1} &= h'_{n-1} + x_nh'_{n-2}, \\ h_n &= x_nh'_{n-1}, \end{aligned}$$

hence $h_i \in \mathbb{C}[h'_1, \dots, h'_{n-1}, x_n]$. Assume that the h_i's are algebraically dependent and let $F(h_1, h_2, \dots, h_n) = 0$ be an algebraic relation of minimal degree. Setting $x_n = 0$ we obtain the relation $F(h'_1, h'_2, \dots, h'_{n-1}, 0) = 0$ between the h'_i, hence $F(z_1, \dots, z_{n-1}, 0) = 0$ by induction. This implies that F is divisible by z_n which contradicts the minimality.

Now let $f \in \mathbb{C}[x_1, \dots, x_n]$ be a symmetric polynomial. Since every homogeneous component of f is symmetric, too, we can assume that f is homogeneous of some degree N. If we write f in the form $f = \sum_i f_i(x_1, \dots, x_{n-1})x_n^i$ then all f_i are symmetric in $x_1, \dots, x_{n-1}$ and so, by induction,

$$f_i \in \mathbb{C}[h'_1, \dots, h'_{n-1}] \subset \mathbb{C}[h_1, \dots, h_{n-1}, x_n].$$

Thus f has the form $f = p(h_1, \dots, h_n) + x_nq(h_1, \dots, h_n, x_n)$ with two polynomials p and q. Again we can assume that $p(h_1, \dots, h_n)$ and $q(h_1, \dots, h_n, x_n)$ are both homogeneous, of degree N and $N-1$, respectively. It follows that $f - p$ is again homogeneous and is divisible by x_n. Since it is symmetric, it is divisible by the product $x_1x_2\dots x_n$, i.e.

$f - p = h_n \overline{f}$ with a symmetric polynomial $\overline{f}$ of degree at most $N - n$. Now the claim follows by induction on the degree of f. □

In the next lectures we will introduce the notion of reflection group, give some examples of reflection groups and state a theorem which shows why reflection groups are so special in invariant theory.

2.2. **Noether's Theorem.** First we claim that $\mathbb{C}[W]^G$ is a subring of $\mathbb{C}[W]$ for any group G. Indeed, assume $f, h \in \mathbb{C}[W]^G$, i.e., $f(x_1, \dots, x_n) = g \cdot f(x_1, \dots, x_n)$ and $h(x_1, \dots, x_n) = g \cdot h(x_1, \dots, x_n)$ for any $g \in G$. Then formulae

$$g \cdot (f - h)(x_1, \dots, x_n) = g \cdot f(x_1, \dots, x_n) - g \cdot h(x_1, \dots, x_n) = f(x_1, \dots, x_n) - h(x_1, \dots, x_n).$$

and

$$g \cdot (fh)(x_1, \dots, x_n) = fh(g \cdot x_1, \dots, g \cdot x_n) = f(g \cdot x_1, \dots, g \cdot x_n)h(g \cdot x_1, \dots, g \cdot x_n) = f(x_1, \dots, x_n)h(x_1, \dots, x_n).$$

show that $f - h$ and fh are also invariants which shows that $\mathbb{C}[W]^G$ is indeed a subring of $\mathbb{C}[W]$.

We say that a subring ring $R \subset \mathbb{C}[x_1, \dots, x_n]$ is finitely generated if there are finitely many $r_1, \dots, r_n \in R$ which generate R, i.e., $R = r_1\mathbb{C}[x_1, \dots, x_n] + \dots + r_n\mathbb{C}[x_1, \dots, x_n]$.

One of the basic results in the invariant theory of finite groups is the following.

Theorem 1 (E. Noether, 1916)**.** *For any representation W of a finite group G the ring of invariants $\mathbb{C}[W]^G$ is generated by the invariants of degree less or equal to the order of G. That is, the number of generators is at most $\binom{|G| + n}{n}$, where $\dim W = n$.*

As an immediate implication of Theorem 1 we have the following result.

Corollary 1. *For any representation W of a finite group G the ring of invariants $\mathbb{C}[W]^G$ is finitely generated.*

One may ask if Corollary 1 holds also for other, not necessarily finite groups. In 1900 David Hilbert presented his famous list of 23 problems on the International Congress of Mathematics in Paris. These problems were very influential for 20th-century mathematics. In particular, Hilbert's fourteenth problem is the following.

Problem 1 (Hilbert's Fourteenth Problem)**.** *Let K be a field and $x_1, \dots, x_n$ algebraically independents elements over K. Let L be a subfield of $K(x_1, \dots, x_n)$ containing K. Is the ring $K[x_1, \dots, x_n] \cap L$ finitely generated over K?*

The motivation for this problem is the following special case, connected with invariant theory.

Problem 2. *Let K be a field and G a subgroup of the full linear group $\mathrm{GL}_n(K)$. Then G acts naturally on polynomials $K[x_1, \dots, x_n]$. Is the ring of invariants $K[x_1, \dots, x_n]^G$ finitely generated over K?*

David Hilbert proved that Corollary 1 (and equivalently Problem 2) holds NOT ONLY for finite groups, but also for the so-called **reductive groups** which we will define later in this course. For example, all classical groups such as GL_n, SL_n, the orthogonal group $\mathrm{O}(n,\mathbb{C})$ and others are reductive.

Remark 2. The counterexample to fourteenth Hilbert's problem was constructed by Nagata in 1958. Actually Nagata found a subgroup $G \subset \mathrm{GL}(W)$, where $W = \mathbb{C}^{32}$, such that $\mathbb{C}[W]^G$ is not finitely generated.

Proof of Theorem 1. Set $N = |G|$ and $\mathbb{C}[W]_{<N} = \{f \in \mathbb{C}[W] \mid \deg f \leq N-1\}$. Let A be the subalgebra of $\mathbb{C}[W]^G$ generated by invariants of degree $\leq N$. Our goal is to prove that $A = \mathbb{C}[W]^G$.

Consider the vector space $B = A \cdot \mathbb{C}[W]_{<N} \subset \mathbb{C}[W]$. Let $\xi \in W^* = \mathbb{C}[W]_1$. Let us prove that $\xi^m \in B$ for any $m \in N$. If $m < N$, then this follows from the definition of B. Next, consider the polynomial

$$\prod_{\sigma \in G} (t - \sigma\xi) = t^N + a_1 t^{N-1} + \cdots + a_N,$$

where $a_i \in \mathbb{C}[W]^G$ and $\deg a_i = i$. Hence $a_i \in A$ for all i. Substituting $t = \xi$, we obtain

$$\xi^N \in A + \xi A + \cdots + \xi^{N-1} A.$$

By induction, we then obtain

$$\xi^m \in A + \xi A + \cdots + \xi^{N-1} A \text{ for any } m \geq N.$$

Therefore, we conclude that $B = \mathbb{C}[W]$.

Now take an arbitrary $f \in \mathbb{C}[W]^G$. As it follows from above f can be written as $\sum_i a_i f_i$, where $a_i \in A$ and $f_i \in \mathbb{C}[W]_{<N}$.

Let $f \mapsto f^*$ denote the (degree-preserving) projection to G-invariants. Then

$$f = f^* = \sum a_i f_i^*,$$

where f_i^* is an invariant of degree $< N$. Hence, $f \in A$, and we are done. □

Remark 3. In connection with Theorem 1, Schmid introduced in a numerical invariant $\beta(G)$ for every finite group G. It is defined to be the minimal number m such that for every representation W of G the invariant ring $\mathbb{C}[W]^G$ is generated by the invariants of degree less or equal to m. By Noether's Theorem above we have $\beta(G) \leq |G|$. Schmid shows that $\beta(G) = |G|$ if and only if G is cyclic. In general, it is rather difficult to calculate $\beta(G)$, except for small groups. For example,

$$\beta(\mathbb{Z}/2 \times \mathbb{Z}/2) = 3,\ \beta(S_3) = 4,\ \beta(S_4) = 10;\ \beta(D_{2n}) = n+1,$$

where D_{2n} denotes the dihedral group of order $2n$. For the symmertic group S_n we can find a lower bound by looking at large cyclic subgroups. Denote by $\gamma(n)$ the maximal order of an element of S_n. Then we have

$$\beta(S_n) \geq \gamma(n) \text{ and } \ln \gamma(n) \sim \sqrt{n \ln n},$$

where $f(n) \sim g(n)$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. In particular, $\beta(S_n)$ grows more rapidly than any power of n.

3. LECTURE 3 (Hilbert-Poincaré series and Molien's theorem).

3.1. **Hilbert-Poincaré series.** Let $V = \bigoplus_{d=0}^{\infty} V_d$ be a direct sum of finite dimensional vector spaces V_d. The Hilbert-Poincaré series $H(V,t)$ is the formal power series in t defined by

$$H(V,t) := \sum_{d=0}^{\infty} \dim(V_d) t^d \tag{2}$$

and encodes in a convenient way the dimensions of the vector spaces V_d. In this lecture, V will usually be the vector space $\mathbb{C}[W]^G$ of polynomial invariants with respect to the action of a group G, where V_d is the subspace of invariants homogeneous of degree d.

Example 6. Taking the polynomial ring in one variable, the Hilbert-Poincaré series is given by

$$H(\mathbb{C}[x],t) = 1 + t + t^2 + \cdots = \frac{1}{1-t}.$$

Similarly, one shows that

$$H(\mathbb{C}[x_1,\ldots,x_n],t) = \sum_{d=0}^{\infty} \binom{d+n-1}{n-1} t^d = \\ (1+t+t^2+\ldots)\ldots(1+t+t^2+\ldots) = \frac{1}{(1-t)^n}.$$

Lemma 1. *Let $f_1,\ldots,f_k \in \mathbb{C}[x_1,\ldots,x_n]$ be algebraically independent homogeneous polynomials, where f_i has degree d_i. Show that the Hilbert-Poincaré series of the subalgebra generated by the f_i is given by*

$$H(\mathbb{C}[f_1,\ldots,f_k],t) = \frac{1}{\prod_{i=1}^{k}(1-t^{d_i})}$$

Proof. Since the polynomials $f_1,\ldots,f_k$ are algebraically independent, the set

$$\{f_1^{i_1} f_2^{i_2} \ldots f_k^{i_k} \mid i_1,i_2,\ldots,i_k \in \mathbb{N} \text{ and } i_1d_1 + i_2d_2 + \ldots i_kd_k = d\}$$

is a basis for the $\mathbb{C}$-vector space $\mathbb{C}[f_1,\ldots,f_n]_d$ of degree d elements in $\mathbb{C}[f_1,\ldots,f_n]$. Hence the dimension of $\mathbb{C}[f_1,\ldots,f_n]_d$ equals the cardinality of the set

$$A_d = \{(i_1,i_2,\ldots,i_k) \in \mathbb{N}^k \mid i_1d_1 + i_2d_2 + \cdots + i_kd_k = d\}.$$

The expansion

$$\frac{1}{\prod_{i=1}^{k}(1-t^{d_i})} = \frac{1}{(1-t^{d_1})}\frac{1}{(1-t^{d_2})}\cdots\frac{1}{(1-t^{d_k})} = \\ (\sum_{i_1=0}^{\infty} t^{i_1d_1})(\sum_{i_2=0}^{\infty} t^{i_2d_2})\ldots(\sum_{i_k=0}^{\infty} t^{i_kd_k}) = \\ \sum_{d=0}^{\infty} \sum_{(i_1,i_2,\ldots,i_k)\in A_d} t^d = \sum_{d=0}^{\infty} |A_d| t^d$$

proves the claim of Lemma 1. □

Example 7. Consider the action of the group G of order 3 on $\mathbb{C}[x,y]$ induced by the linear map $x \mapsto \xi_3 x,\ y \mapsto \xi_2^{-1}$, where ξ_3 is a third root of unity. By Example 3, $\mathbb{C}[x,y]^G = \mathbb{C}[x^3, y^3, xy]$. In fact, x^3 and y^3 are algebraically independent, and

$$\mathbb{C}[x,y]^G = \mathbb{C}[x^3,y^3] \oplus \mathbb{C}[x^3,y^3]xy \oplus \mathbb{C}[x^3,y^3](xy)^2$$

Since $H(\mathbb{C}[x^3,y^3],t) = \frac{1}{(1-t^3)^2}$, we obtain

$$H(\mathbb{C}[x,y]^G,t) = \frac{1+t^2+t^4}{(1-t^3)^2}.$$

Exercise 1. *Compute the Hilbert-Poincaré series of* $\mathbb{C}[x^2,y^2,xy]$.

3.2. **Molien's theorem.** For finite groups G that acts on $\mathbb{C}[W] = \mathbb{C}[x_1,\dots,x_n]$, it is possible to compute the Hilbert-Poincaré series of $\mathbb{C}[x_1,\dots,x_n]^G$ directly, without prior knowlegde about the generators. This is captured in the following beautiful theorem of Molien.

Theorem 2 (Molien's Theorem)**.** *Let* $\rho\colon G \to \mathrm{GL}(W)$ *be a representation of a finite group on a finite dimensional vector space* W*. Then the Hilbert-Poincaré series of* $\mathbb{C}[W]^G$ *is given by*

$$H(\mathbb{C}[W]^G,t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{Id}-\rho(g)t)}. \tag{3}$$

Before starting the proof of the theorem we need the following remark.

Remark 4. if $g \in \mathrm{GL}(W)$ is a matrix of finite order k, then we claim that g is **diagonalizable**, i.e., there exists $h \in \mathrm{GL}(W)$ such that hgh^{-1} is diagonal. Indeed, since $g^k = 1$, we have that the minimal polynomial $p_g(t)$ divides $x^k - 1$. Since all roots of $x^k - 1$ are different, all roots of $p_g(t)$ are different too. Therefore, from the course of Linear Algebra we conclude that g is diagonalizable.

Proof of Theorem 2. Consider the action of G on $\mathbb{C}[W]$ induced by the representation ρ. Denote for $g \in G$ and $d \in \mathbb{N}$ by $L_d(g) \in \mathrm{GL}(\mathbb{C}[W]_d)$ the linear map corresponding to the action of $g \in G$ on the homogeneous polynomials $\mathbb{C}[W]_d$ of degree d. So $L_1(g) = \rho^*(g)$.

The linear map

$$\pi_d := \frac{1}{|G|}\sum_{g\in G} L_d(g)\colon \mathbb{C}[W]_d \to \mathbb{C}[W]_d$$

is a projection onto $\mathbb{C}[W]_d^G$. That is, $\pi_d(p) \in \mathbb{C}[W]_d^G$ for all $p \in \mathbb{C}[W]_d$ and π_d is the identity on $\mathbb{C}[W]_d^G$. It follows that $\mathrm{tr}(\pi_d) = \dim(\mathbb{C}[W]_d^G)$ (please, check this equality). This gives:

$$H(\mathbb{C}[W]^G,t) = \frac{1}{|G|}\sum_{g\in G}\sum_{d=0}^{\infty}\mathrm{tr}(L_d(g))t^d. \tag{4}$$

Now lets fix an element $g \in G$ and compute the inner sum $\sum_{d=0}^{\infty}\mathrm{tr}(L_d(g))t^d$. From Remark 4 it follows that there exists a basis $x_1,\dots,x_n$ of W^* that is a system of

eigenvectors for $L_1(g)$, say $L_1(g)x_i = \lambda_i x_i$. Then the monomials in $x_1, \ldots, x_n$ of degree d form a system of eigenvectors of $L_d(g)$ with eigenvalues given by:

$$L_d(g)x_1^{d_1} \ldots x_n^{d_n} = \lambda_1^{d_1} \ldots \lambda_n^{d_n} x_1^{d_1} \ldots x_n^{d_n}$$

for all $d_1 + \cdots + d_n = d$. It follows that

$$\sum_{d=0}^{\infty} \operatorname{tr}(L_d(g))t^d = (1 + \lambda_1 t + \lambda_1^2 t + \ldots) \ldots (1 + \lambda_n t + \lambda_n t^2 + \ldots) = \tag{5}$$

$$\frac{1}{1-\lambda_1 t} \cdots \frac{1}{1-\lambda_n t} = \frac{1}{\det(\mathrm{Id} - L_1(g)t)}. \tag{6}$$

Using the fact that for every g the equality $\det(\mathrm{Id} - L_1(g)t) = \det(\mathrm{Id} - \rho(g^{-1})t)$ holds and combining equations (4) and (5)-(6), we arrive at

$$H(\mathbb{C}[W]^G, t) = \frac{1}{|G|} \sum_{g \in G} \sum_{d=0}^{\infty} \operatorname{tr}(L_d(g)) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - \rho(g^{-1})t)} = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(\mathrm{Id} - \rho(g)t)},$$

where the last equality follows by changing the order in which we sum over G. This completes the proof. □

Example 8. Consider again the action of a cyclic group G of order 3 on $\mathbb{C}[x, y]$ induced by the linear map $x \mapsto \xi x$, $y \mapsto \xi^{-1} y$, where ξ is a third root of unity. Using Molien's theorem, we find

$$H(\mathbb{C}[x, y]^G, t) = \frac{1}{3} \left(\frac{1}{(1-t)(1-t)} + \frac{1}{(1-\xi t)(1-\xi^2 t)} + \frac{1}{(1-\xi^2 t)(1-\xi t)} \right).$$

A little algebraic manipulation and the fact that

$$(1 - \xi t)(1 - \xi^2 t) = (1 - (\xi + \xi^2)t + \xi^3 t^2) = (1 + t + t^2)$$

(as $\xi^3 = 1$ and hence the expression $0 = \xi^3 - 1 = (\xi - 1)(\xi^2 + \xi + 1)$ implies that $\xi^2 + \xi + 1 = 0$) shows that

$$H(\mathbb{C}[x, y]^G, t) = \frac{(1 - t + t^2)(1 + t + t^2)}{(1-t)^2(1-\xi t)^2(1-\xi^2 t)^2} = \frac{1 + t^2 + t^4}{(1-t^3)^2}$$

Since this is equal to the Hilbert-Poincaré series of $\mathbb{C}[x^3, y^3, xy]$ (see Example 7), we obtain as a byproduct that the invariant ring is indeed generated by the three invariants x^3, y^3 and xy.

Exercise 2. *Let G be the matrix group generated by $A, B \in \mathrm{GL}_2$ given by*

$$A := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Use Molien's theorem to prove that the Hilbert series of $\mathbb{C}[x, y]^G$ is given by

$$H(\mathbb{C}[x, y]^G, t) = \frac{1 + t^6}{(1 - t^4)^2}.$$

Find algebraically independent invariants f_1, f_2 of degree 4 and a third invariant f_3 of degree 6, such that $\mathbb{C}[x,y]^G = \mathbb{C}[f_1,f_2] \oplus \mathbb{C}[f_1,f_2]f_3$.

4. LECTURE 4 (Brief Introduction to Commutative Algebra and Algebraic Geometry).

Three of Hilbert's fundamental contributions to modern algebra, namely, the Nullstellensatz, the Basis Theorem and the Syzygy Theorem, were first proved as lemmas in his invariant theory papers from 1890 and 1893. In this course we will need first two from these three theorems which we present in this section.

We start with introducing a so-called Zariski topology.

4.1. Zero sets and Zariski topology.

We now define the basic object of algebraic geometry, namely the zero set of regular functions. Let W be a finite dimensional vector space.

Definition 4. If $f \in \mathbb{C}[W]$, then we define the **zero set** of f by zero set

$$\mathcal{V}(f) := \{w \in W \mid f(w) = 0\} = f^{-1}(0).$$

More generally, the zero set of $f_1, f_2, \dots, f_s \in \mathbb{C}[W]$ or of a subset $S \subset \mathbb{C}[W]$ is defined by

$$\mathcal{V}(f_1, f_2, \dots, f_s) := \cap_{i=1}^{w} \mathcal{V}(f_i) = \{w \in W \mid f_1(w) = \dots = f_s(w) = 0\}$$

or

$$\mathcal{V}(S) := \{w \in W \mid f(w) = 0 \text{ for all } f \in S\}$$

Remark 5. The following properties of zero sets follow immediately from the definition.

(1) Let $S \subseteq \mathbb{C}[W]$ and denote by $\mathfrak{a} = (S) \subseteq \mathbb{C}[W]$ the ideal generated by S. Then $\mathcal{V}(S) = \mathcal{V}(\mathfrak{a})$.

(2) If $S \subseteq T \subset \mathbb{C}[W]$, then $\mathcal{V}(S) \supseteq \mathcal{V}(T)$.

(3) For any family $(S_i)_{i \in I}$ of subset $S_i \subset \mathbb{C}[W]$ we have

$$\mathcal{V}(\cup_{i \in \mathcal{I}} S_i) = \cap_{i \in \mathcal{I}} \mathcal{V}(S_i).$$

Lemma 2. *Let W be a finite dimensional vector space and let $\mathfrak{a}, \mathfrak{b}$ be ideals in $\mathcal{O}(W)$ and $(\mathfrak{a}_i \mid i \in \mathcal{I})$ a family of ideals of $\mathbb{C}[W]$.*

(1) *If $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathcal{V}(\mathfrak{a}) \supseteq \mathcal{V}(\mathfrak{b})$.*

(2) $\cap_{i \in \mathcal{I}} \mathcal{V}(\mathfrak{a}_i) = \mathcal{V}(\sum_{i \in \mathcal{I}} \mathfrak{a}_i)$.

(3) $\mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}) = \mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{V}(\mathfrak{a} \cdot \mathfrak{b})$.

(4) $\mathcal{V}(0) = W$ *and* $\mathcal{V}(1) = \emptyset$.

Proof. Properties (1) and (2) follow from Remark 5, and property (4) is easy. So we are left with property (3). Since $\mathfrak{a} \supseteq \mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{a} \cdot \mathfrak{b}$, it follows from (1) that $\mathcal{V}(\mathfrak{a}) \subseteq \mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathcal{V}(\mathfrak{a} \cdot \mathfrak{b})$. So it remains to show that $\mathcal{V}(\mathfrak{a} \cdot \mathfrak{b}) \subseteq \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b})$. If $v \in W$ does not belong to $\mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b})$, then there are functions $f \in \mathfrak{a}$ and $h \in \mathfrak{a}$ such that $f(v) \neq 0 \neq h(v)$. Since $fh \in \mathfrak{a} \cdot \mathfrak{b}$ and $(fh)(v) \neq 0$ we see that $v \notin \mathcal{V}(\mathfrak{a} \cdot \mathfrak{b})$, and the claim follows. □

Definition 5. The lemma shows that the subsets $\mathcal{V}(\mathfrak{a})$ where $\mathfrak{a}$ runs through the ideals of $\mathbb{C}[W]$ form the closed sets of topology on W which is called **Zariski** topology. From now on all topological terms like "open", "closed", "neighborhood", "continuous", etc. will refer to the Zariski topology.

Example 9. (0) Let us consider the vector space of all matrices

$$\mathrm{M}_n(\mathbb{C}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & & \dots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \mid a_{ij} \in \mathbb{C}, \text{ where } 1 \le i,j \le n \right\}.$$

This is the vector space of dimension n^2.

(1) The subset $\mathrm{SL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ of those matricies which have determinant 1 is the closed subset in Zariski topology. Indeed,

$$\mathrm{SL}_n(\mathbb{C}) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & & \dots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \in \mathrm{M}_n(\mathbb{C}) \mid \det A - 1 = 0 \right\}.$$

Since $\det A$ is a polynomial in variables a_{ij}, where $1 \le i,j \le n$, we have that $\mathrm{SL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ is a closed subset.

(2) Consider the closed subset

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_n(\mathbb{C}) \mid b, c = 0,\ ad = 1 \right\}$$

of the vector space $\mathrm{M}_2(\mathbb{C})$. It is easy to see that S can be identified with $\mathbb{C}^*$. Therefore, $\mathbb{C}^*$ is a closed subset of $\mathrm{M}_2(\mathbb{C})$.

Definition 6. Let $X \subset W$ be a closed subset. A regular function on X is defined to be the restriction of a regular function on W:

$$\mathbb{C}[X] := \{ f \mid_X \mid f \in \mathbb{C}[W] \}.$$

The kernel of the (surjective) restriction map $\mathrm{res} : \mathbb{C}[W] \to \mathbb{C}[X]$ is called the vanishing ideal of X, or shortly the ideal of X:

$$I(X) := \{ f \in \mathbb{C}[W] \mid f(x) = 0 \text{ for all } x \in X \}.$$

Thus, we have a canonical isomorphism $\mathbb{C}[W]/I(X) \xrightarrow{\sim} \mathbb{C}[X]$ of rings.

4.2. **Hilbert's Nullstellensatz.** The famous Nullstellensatz of Hilbert appears in many different forms which are all more or less equivalent. We will give some of them in this section.

Definition 7. If $\mathfrak{a}$ is an ideal of an arbitrary ring R, its **radical** $\sqrt{\mathfrak{a}}$ is defined by

$$\sqrt{\mathfrak{a}} := \{ r \in R \mid r^m \in \mathfrak{a} \text{ for some } m > 0 \}.$$

Clearly, $\sqrt{\mathfrak{a}}$ is an ideal and $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. Moreover, $\sqrt{\mathfrak{a}} = R$ implies that $\mathfrak{a} = R$. The ideal $\mathfrak{a}$ is called **radical** if $\mathfrak{a} = \sqrt{\mathfrak{a}}$. The ring R is called **reduced** if $\sqrt{(0)} = (0)$, or, equivalently, if R contains no nonzero nilpotent elements. Also, if $\mathfrak{a} \subset \mathbb{C}[W]$ is an ideal, then $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\sqrt{\mathfrak{a}})$, hence $I(X)$ is radical for every $X \subseteq W$.

Theorem 3 (Hilbert's Nullstellensatz)**.** *Let $\mathfrak{a} \subseteq \mathbb{C}[W]$ be an ideal and $X := \mathcal{V}(\mathfrak{a}) \subset W$ its zero set. Then*

$$I(X) = I(\mathcal{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

A first consequence is that every proper ideal has a non-empty zero set, because $X = \mathcal{V}(\mathfrak{a}) = \emptyset$ implies that $\sqrt{\mathfrak{a}} = I(X) = \mathbb{C}[W]$ and so $\mathfrak{a} = \mathbb{C}[W]$.

Corollary 2. *For every ideal $\mathfrak{a} \neq \mathbb{C}[W]$ we have $\mathcal{V}(\mathfrak{a}) \neq \emptyset$.*

Let $\mathfrak{m} \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be a maximal ideal and $\mathfrak{a} = (a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{m})$ which exists by the previous corollary. Then $\mathfrak{m} \subseteq (x_1 - a_1, \ldots, x_n - a_n)$, and so these two are equal.

Corollary 3. *Every maximal ideal $\mathfrak{m}$ of $\mathbb{C}[x_1, \ldots, x_n]$ is of the form*

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n).$$

Exercise 3. *Let $\mathfrak{a} \subset R$ be an ideal of a (commutative) ring R. Then $\mathfrak{a}$ is perfect if and only if the residue class ring $R/\mathfrak{a}$ has no nilpotent elements different from 0.*

Proof of Theorem 3. We first prove Corollary 3. It also implies Corollary 2, because every proper ideal is contained in a maximal ideal.

Let $\mathfrak{m} \subset \mathbb{C}[x_1, \ldots, x_n]$ be a maximal ideal and denote by $K = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m}$ its residue class field. Then K contains $\mathbb{C}$ and has a countable $\mathbb{C}$-basis, because $\mathbb{C}[x_1, \ldots, x_n]$ does. If $K \neq \mathbb{C}$ and $p \in K \setminus \mathbb{C}$, then p is transcendental over $\mathbb{C}$. It follows that the elements $(\frac{1}{p-a} \mid a \in \mathbb{C})$ from K form a non-countable set of linearly independent elements over $\mathbb{C}$. This contradiction shows that $K = \mathbb{C}$. Thus $x_i + \mathfrak{m} = a_i + \mathfrak{m}$ for a suitable $a_i \in \mathbb{C}$ (for $i = 1, \ldots, n$), and so $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$. This proves Corollary 3.

To get the theorem, we use the so-called trick of **Rabinowich**. Let $\mathfrak{a} \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal and assume that the polynomial f vanishes on $\mathcal{V}(\mathfrak{a})$. Now consider the polynomial ring $R = \mathbb{C}[x_0, x_1, \ldots, x_n]$ in $n+1$ variables and the ideal $\mathfrak{b} = (\mathfrak{a}, 1 - x_0 f) \subset R$ generated by $1 - x_0 f$ and the elements of $\mathfrak{a}$. Clearly, $\mathcal{V}(\mathfrak{b}) = \emptyset$ and so $1 \in \mathfrak{b}$, by Corollary 2. This means that we can find an equation of the form

$$\sum_i h_i f_i + h(1 - x_0 f) = 1$$

where $f_i \in \mathfrak{a}$ and $h_i, h \in R$. Now we substitute $\frac{1}{f}$ for x_0 and find

$$\sum_i h_i(\frac{1}{f}, x_1, \ldots, x_n) f_i = 1.$$

Clearing denominators finally gives $\sum_i \tilde{h}_i f_i = f^m$ for some $m \in \mathbb{N}$, i.e., $f^m \in \mathfrak{a}$, and the claim follows. □

Corollary 4. *For any ideal $\mathfrak{a} \subset \mathbb{C}[W]$ and its zero set $X = \mathcal{V}(\mathfrak{a})$ we have*

$$\mathbb{C}[X] = \mathbb{C}[W]/\sqrt{\mathfrak{a}}.$$

Example 10. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be an arbitrary polynomial and consider its decomposition into irreducible factors: $f = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$. Then $\sqrt{(f)} = (p_1 p_2 \ldots p_s)$ and so the ideal (f) is radical if and only if the polynomial f is square-free. In particular, if $f \in \mathbb{C}[x_1, \ldots, x_n]$ is irreducible, then $\mathbb{C}[\mathcal{V}(f)] = \mathbb{C}[x_1, \ldots, x_n]/(f)$. A closed subset of the form $\mathcal{V}(f)$ is called a hypersurface.

Exercise 4. *If $X \subset V$ is a closed subset and $\mathfrak{m} \subset \mathbb{C}[X]$ a maximal ideal, then $\mathbb{C}[X]/\mathfrak{m} = \mathbb{C}$. Moreover, $\mathfrak{m} = \ker(\mathrm{ev}_x \colon f \mapsto f(x))$ for a suitable $x \in X$.*

4.3. **Hilbert Basis Theorem.**

Definition 8. A ring R is called Noetherian if every ideal in R is finitely generated, i.e. is of the form $(a_1, a_2, \ldots, a_n)$ for some $a_1, a_2, \ldots, a_n \in R$.

Lemma 3. *Let R be a commutative ring. Then, R is Noetherian if and only if every ascending chain of ideals*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

in R stabilizes, i.e there exists $m \in \mathbb{N}$ with $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \ldots$

Proof. Assume R is Noetherian. Given an ascending chain of ideals in R

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

Let $\mathfrak{a} = \cup_{n=1}^{\infty} \mathfrak{a}_n$. It is routine to check that $\mathfrak{a}$ is an ideal. Since $\mathfrak{a}$ is finitely generated, $\mathfrak{a} = (a_1, a_2, \ldots, a_s)$, and so there exists $m \in N$ such that $a_1, a_2, \ldots, a_s \in \mathfrak{a}_m$. Now it is clear that $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \ldots$ and so the chain stabilizes, as desired. Conversely, assume $\mathfrak{a} \subseteq R$ is an ideal. We want to show that $\mathfrak{a}$ is finitely generated ideal. Choose $a_1 \in \mathfrak{a}$ and set $\mathfrak{a}_1 = (a_1)$. If $\mathfrak{a} = \mathfrak{a}_1$, we are done. Otherwise, choose $a_2 \in \mathfrak{a} \setminus \mathfrak{a}_1$ and set $\mathfrak{a}_2 = (a_1, a_2)$. Proceed to define $a_2, a_3, \ldots$ in this manner, and set $\mathfrak{a}_n = (a_1, a_2, \ldots, a_n)$. If $\mathfrak{a} = \mathfrak{a}_n$ for some $n \in \mathbb{N}$, then we are done. Otherwise,

$$\mathfrak{a}_1 \supsetneq \mathfrak{a}_2 \supsetneq \mathfrak{a}_3 \supsetneq \ldots$$

is a strictly ascending chain of ideals, contradiction. □

Example 11. (1) a field is the example of a Noetherian ring as it has only two ideals.
(2) The polynomial ring in infinitely many variables $R[x_1, x_2, \ldots]$ is **not** Noetherian.

Theorem 4 (Hilbert Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian too.*

Proof. Assume, to the contrary, that there exists an ideal $\mathfrak{a} \subseteq R[x]$ which is not finitely generated. Then, $\mathfrak{a} \neq (0)$. Choose an element $f(x) \in \mathfrak{a}$ of minimal degree, with degree d_1. Set $\mathfrak{a}_1 = (f_1) \subset R[x]$. Since $\mathfrak{a}$ is not finitely generated, $\mathfrak{a} \neq \mathfrak{a}_1$. Choose $f_2(x) \in \mathfrak{a} \setminus \mathfrak{a}_1$ of minimal degree d_2. Set $\mathfrak{a}_2 = (f_1, f_2)$. Continue to define $f_3, f_4, \ldots$ in this manner. Note that $d_1 \leq d_2 \leq d_3 \leq \ldots$. Let a_i be the leading coefficient of $f_i(x)$. Then,

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

is an ascending chain of ideals in R. Thus, $a_{m+1} \in (a_1, a_2, \ldots, a_m)$ for some $m \in \mathbb{N}$. In other words,

$$a_{m+1} = r_1 a_1 + r_2 a_2 + \cdots + r_m a_m$$

for some $r_1, r_2, \ldots, r_m \in R$. Now, set

$$g_{m+1} = f_{m+1} - \sum_{i=1}^{m} r_i x^{d_{m+1} - d_i} f_i.$$

The x^{d_m+1} term cancels out, and this polynomial g_{m+1} has a degree strictly less than d_{m+1}. On the other hand, $g_{m+1} \notin \mathfrak{a}_m$, because otherwise it would imply $f_{m+1} \in \mathfrak{a}_m$

which would be a contradiction. The fact that $g_{m+1} \notin \mathfrak{a}_m$ contradicts the minimality of degree of f_{m+1}. □

5. LECTURE 5 (Reflection Groups and their invariants).

Definition 9. A (complex) **reflection** σ (sometimes also called pseudoreflection or unitary reflection) of a finite-dimensional complex vector space W is an element $\sigma \in \mathrm{GL}(W)$ of finite order that fixes a complex hyperplane pointwise, that is, the fixed-space $\mathrm{Fix}(\sigma) = \ker(\sigma - \mathrm{Id}_W)$ has codimension 1.

A (finite) **reflection group** G is a finite subgroup of $\mathrm{GL}(W)$ that is generated by reflections.

In the next lecture we will prove the following result.

Theorem 5 (Shephard-Todd-Chevalley, 1954)**.** *For any representation W of a finite group G the ring of invariants $\mathbb{C}[W]^G$ is isomorphic to a polynomial ring if and only if G is a reflection group.*

Theorem 5 was first proved for real reflection groups by **Shephard** and **Todd** in 1954, and subsequently generalized to the complex case by **Chevalley** in 1955.

Consider now a few classical examples of reflection groups.

Example 12. Let $G \subset \mathrm{GL}(\mathbb{C}^2)$ be a subgroup generated by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. From Example 1 it follows that G is a reflection group as $\mathrm{Fix}(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$ is a one-dimensional vector subspace of $\mathbb{C}^2$.

Example 13. Let S_n be the symmetric group that acts on n-dimensional vector space $W = \mathbb{C}^n$ in the following way: $(i, j) \in S_n$ acts on W by permuting i-th and j-th coordinates. By Proposition 1 we have that $\mathbb{C}[x_1, x_2, \ldots, x_n]^{S_n}$ is generated by n elements. Hence, by Theorem 5, S_n is a reflection group.

Now let us show directly that S_n is a reflection group. Indeed, since S_n is generated by elements of the form (i, j), where $i, j \in \{1, \ldots, n\}$, $i < j$ and

$$\mathrm{Fix}((i, j)) = \{(a_1, \ldots, a_n) \mid a_i = a_j\}$$

is a hyperplane in $W = \mathbb{C}^n$ we conclude that S_n is a reflection group.

Example 14. Let $G = D_k$ be the dihedral group, i.e., the group of symmetries of a regular k-gon centerd at the origin. As a subgroup of GL_2 (which naturally acts on two-dimenisoanl vector space $\mathbb{C}^2$), it is generated by

$$r_k = \begin{pmatrix} \cos(2\pi/k) & -\sin(2\pi/k) \\ \sin(2\pi/k) & \cos(2\pi/k) \end{pmatrix}, \; s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus, $D_k = \{r_k^i s^j \mid i = 0, 1, 2, \ldots, k-1; \; j = 1, 2\}$. It is easy to see that D_k is generated by s and $r_k s$. Moreover, both s and $r_k s$ have order 2 and

$$\mathrm{Fix}(s) = \{(a, 0) \mid a \in \mathbb{C}\}$$

and

$$\mathrm{Fix}(rs) = \{(r_{2k}\begin{pmatrix} a \\ 0 \end{pmatrix})^t \mid a \in \mathbb{C}\},$$

where $\begin{pmatrix} c \\ d \end{pmatrix}^t$ means the transpose vector (c, d). Therefore, both $\mathrm{Fix}(s)$ and $\mathrm{Fix}(xs)$ are one-dimenional vector subspaces in $\mathbb{C}^2$ which implies that D_k is the reflection group.

Exercise 5. *Let the dihedral group $G = \langle r_k, s\rangle \simeq D_k$ acts on $\mathbb{C}[x, y]$ in the follwoing way: let $\xi_k := exp(\frac{2\pi i}{k}) \in \mathbb{C}^*$ be a k-th primitive root of unity, and let*

$$\rho_k \colon G \to \mathrm{GL}_2(\mathbb{C}) \colon r_k \mapsto \begin{pmatrix} \xi_k & 0 \\ 0 & \xi_k^{-1} \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

be a representation of G. Prove that $\mathbb{C}[x_1, x_2]^{D_k} = \mathbb{C}[x_1x_2, x_1^k + x_2^k]$.

For the proof of Theorem 5 we will need a so-called **Reynolds operator** which we define in the following way:

$$* \colon \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]^G, f \mapsto f^* = \frac{1}{|G|} \sum_{g \in G} g \cdot f.$$

The following proposition follows immediately from the definition of Reynolds operator.

Proposition 2. *The Reynolds operator $*$ has the following properties.*

(a) $*$ is a $\mathbb{C}$-linear map, i.e., $(\lambda f + \mu h)^* = \lambda f^* + \mu h^*$ for all $f, h \in \mathbb{C}[x_1, \ldots, x_n]$ and $\lambda, \mu \in \mathbb{C}$.

(b) $*$ restricts to the identity map on $\mathbb{C}[x_1, \ldots, x_n]^G$, i.e., $f = f^*$ for all invariants $f \in \mathbb{C}[x_1, \ldots, x_n]^G$.

(c) $(hf)^* = h^*f$ for all $h \in \mathbb{C}[x_1, \ldots, x_n]$ and $f \in \mathbb{C}[x_1, \ldots, x_n]^G$.

Now we start with some lemmata in order to prove Theorem 5. Let $\sigma \in \mathrm{GL}(\mathbb{C}^n)$ be any reflection. Then the kernel of the linear transformation $\sigma - \mathrm{Id}$ is a hyperplane H_σ in $W = \mathbb{C}^n$. Let L_σ denote the linear polynomial whose zero set is the hyperplane H_σ.

Lemma 4. *For all polynomials $f \in \mathbb{C}[x_1, \ldots, x_n]$, the linear polynomial L_σ is a divisor of $\sigma f - f$.*

Proof. Given $v \in \mathbb{C}^n$ with $L_\sigma(v) = 0$, we have

$$v \in H_\sigma f \Rightarrow \sigma v = v \Rightarrow f(\sigma v) = f(v) \Rightarrow (\sigma f - f)(v) = 0.$$

Since the linear polynomial L_σ is irreducible, Hilbert's Nullstellensatz implies that $\sigma f - f$ is a multiple of L_σ. □

In the following let $G \subset \mathrm{GL}(\mathbb{C}^n)$ be a finite reflection group. Let I_G denotes the ideal in $\mathbb{C}[x_1, \ldots, x_n]$ which is generated by all homogeneous invariants of positive degree.

Proposition 3. *Let $h_1, h_2, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n]$ be homogeneous polynomials, let $f_1, f_2, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]^G$ be invariants, and suppose that $f_1h_1 + f_2h_2 + \cdots + f_mh_m = 0$. Then either $h_1 \in I_G$, or f_1 is contained in the ideal $\langle f_2, \ldots, f_m\rangle$ in $\mathbb{C}[x_1, \ldots, x_n]$.*

Proof. We proceed by induction on the degree of h_1. If $h_1 = 0$, then $h_1 \in I_G$. If $\deg h_1 = 0$, then h_1 is a constant and hence $f_1 \in \langle f_2, \dots, f_m \rangle$. We may therefore assume $\deg h_1 > 0$ and that the assertion is true for smaller degrees. Suppose that $f_1 \notin \langle f_2, \dots, f_m \rangle$.

Let $\sigma \in G$ be any reflection. Then

$$\sum_{i=1}^{m} f_i \sigma(h_i) = \sigma(\sum_{i=1}^{m} f_i h_i) = \sigma(0) = 0.$$

By Lemma 4, we can write $\sigma h_i = h_i + L_\sigma \tilde{h}_i$, where $\tilde{h}_i$ is a homogeneous polynomial of degree $\deg h_i - 1$. We get

$$0 = \sum_{i=1}^{m} g_i(h_i + L_\sigma \tilde{h}_i) = L_\sigma(\sum_{i=1}^{m} f_i \tilde{h}_i),$$

and consequently $f_1\tilde{h}_1 + f_2\tilde{h}_2 + \cdots + f_m\tilde{h}_m = 0$. By the induction hypothesis, we have $\tilde{h}_1 \in I_G$, and therefore $\sigma h_1 - h_1 = \tilde{h}_1 L_\sigma \in I_G$.

Now let $\pi = \sigma_1\sigma_2 \dots \sigma_l$ be an arbitrary element of G, written as a product of reflections. Since the ideal I_G is invariant under the action of G,

$$\pi h_1 - h_1 = \sum_{i=0}^{l-1} (\sigma_0 \dots \sigma_i \sigma_{i+1} h_1 - \sigma_0 \dots \sigma_i h_1) = \sum_{i=0}^{l-1} (\sigma_0 \dots \sigma_i)(\sigma_{i+1} h_1 - h_1) \in I_G,$$

where σ_0 is the identity element of G. This implies that

$$\frac{1}{|G|} \sum_{\pi \in G} (\pi h_1 - h_1) = \frac{1}{|G|} \sum_{\pi \in G} (\pi h_1) - h_1 \in I_G$$

and consequently since $\frac{1}{|G|} \sum_{\pi \in G} (\pi h_1) \in I_G$ (please, check this) we conclude that $h_1 \in I_G$. □

In the next lecture we will prove Theorem 5.

6. LECTURE 6 (Proof of Theorem 5).

Proof of Theorem 5 (if-part). By Hilbert's basis theorem, there exists a finite set $\langle f_1, f_2, \dots, f_m \rangle \subset \mathbb{C}[x_1, \dots, x_n]$ of homogeneous invariants which generates the ideal I_G. We claim that

$$\mathbb{C}[x_1, \dots, x_n]^G = \mathbb{C}[f_1, \dots, f_m]. \tag{7}$$

Indeed, assume the contrary, let f be a homogeneous element of minimum degree in $\mathbb{C}[x_1, \dots, x_n]^G \setminus \mathbb{C}[f_1, f_2, \dots, f_m]$. Since $f \in I_G$, we have $f = \sum_{j=1}^{s} h_j f_j$ for some homogeneous polynomials $h_j \in \mathbb{C}[x_1, \dots, x_n]$ of degree less than $\deg f$. Applying the Reynolds operator on both sides of this equation we get

$$f = f^* = (\sum_{j=1}^{s} h_j f_j)^* = \sum_{j=1}^{s} h_j^* f_j$$

by Proposition 2. The new coefficients h_j^* are homogeneous invariants whose degree is less than $\deg f$. From the minimality assumption on f we get $h_j^* \in \mathbb{C}[f_1, \ldots, f_m]$ and therefore $f \in \mathbb{C}[f_1, \ldots, f_m]$, which is a contradiction to our assumption. This proves (7).

Suppose now that m is minimal with the property that $I_G = \langle f_1, \ldots, f_m \rangle$, i.e., no smaller set of homogeneous invariants generates I_G. We need to prove that $m = n$, or, equivalently, that the invariants $f_1, f_2, \ldots, f_m$ are algebraically independent over $\mathbb{C}$.

Our proof is by contradiction. Suppose there exists a nonzero polynomial $F \in \mathbb{C}[y_1, y_2, \ldots, y_m]$ such that $F(f_1, f_2, \ldots, f_m) = 0$ in $\mathbb{C}[x_1, \ldots, x_n]$. We may assume that F is of minimal degree and that all monomials $x^{i_1} x^{i_2} \ldots x_n^{i_n}$ occurring (before cancellation) in the expansion of $F(f_1, f_2, \ldots, f_m)$ have the same degree $d = i_1 + i_2 + \ldots i_n$.

For $i = 1, 2, \ldots, m$ consider the invariant

$$F_i = \frac{\partial F}{\partial y_i}(f_1, f_2, \ldots, f_m) \in \mathbb{C}[x_1, \ldots, x_n]^G.$$

Each F_i is either 0 or of degree $d - \deg f_i$. Since $F(y_1, \ldots, y_m)$ is not a constant, there exists an i with $\frac{\partial F}{\partial y_i}(y_1, y_2, \ldots, y_m) \neq 0$, and hence, $F_i \neq 0$, by the choice of F.

Let J denote the ideal in $\mathbb{C}[x_1, \ldots, x_n]$ generated by $\langle F_1, F_2, \ldots, F_m \rangle$, and relabel if necessary so that J is generated by $\langle F_1, \ldots, F_k \rangle$ but no proper subset. For $i = k+1, \ldots, m$ write $F_i = \sum_{j=1}^{k} h_{ij} F_j$, where h_{ij} is either 0 or homogeneous of degree $\deg F_i - \deg F_j = \deg f_j - \deg f_i$. We have

$$0 = \frac{\partial}{\partial x_s}(F(f_1, f_2, \ldots, f_m)) = \sum_{i=1}^{m} F_i \frac{\partial f_i}{\partial x_s} = \sum_{i=1}^{k} F_i \frac{\partial f_i}{\partial x_s} + \sum_{i=k+1}^{m} (\sum_{j=1}^{k} h_{ij} F_j) \frac{\partial f_i}{x_s} =$$
$$\sum_{i=1}^{k} F_i (\frac{\partial f_i}{\partial x_s} + \sum_{j=k+1}^{m} h_{ji} \frac{\partial f_j}{\partial x_s}).$$

Since $F_1 \notin \langle F_2, \ldots, F_k \rangle$, Proposition 3 implies

$$\frac{\partial f_1}{\partial x_s} + \sum_{j=k+1}^{m} h_{j1} \frac{\partial f_j}{\partial x_s} \in I_G \text{ for } s = 1, \ldots, n.$$

Multiplying with x_s and summing over s, we can apply Euler's formula to find

$$\sum_{s=1}^{n} x_s \frac{\partial f_1}{\partial x_s} + \sum_{j=k+1}^{m} h_{j1} \sum_{s=1}^{n} x_s \frac{\partial f_j}{\partial x_s} = (\deg f_1) f_1 + \sum_{j=k+1}^{m} h_{j1} (\deg f_j) f_j \in$$
$$\langle x_1, \ldots, x_n \rangle I_G \subset \langle x_1 f_1, \ldots, x_n f_n \rangle + \langle f_2, \ldots, f_m \rangle.$$

All monomials in this polynomial are of degree $\deg(f_1)$, and therefore

$$\deg(f_1) f_1 + \sum_{j=k+1}^{m} h_{j1} (\deg f_j) f_j \in \langle f_2, \ldots, f_m \rangle.$$

The last expression implies $f_1 \in \langle f_2, \ldots, f_m \rangle$, which is a contradiction to the minimality of m. This completes the proof of the "if"-part of Theorem 5. □

Remark 6. The first paragraph of (if-part) proof of Theorem 5 implies the remarkable statement that every ideal basis $\{f_1, \ldots, f_m\}$ of homogeneous elements of I_G is automatically an algebra basis for $\mathbb{C}[x_1, \ldots, x_n]^G$.

There is a simple criterion for the algebraic independence of n polynomials $f_1, \ldots, f_n$ in n indeterminates $x_1, \ldots, x_n$, expressed in terms of the Jacobian determinant. We will need this in (only if-part) of the proof of Theorem 5. Write $\mathrm{jac}(f_1, \ldots, f_n)$ for the determinant of the $n \times n$ matrix whose (i, j)-entry is $\frac{\partial f_i}{\partial x_j}$.

Proposition 4 (Jacobian Criterion)**.** *The polynomials $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n]$ are algebraically independent if and only if* $\mathrm{jac}(f_1, \ldots, f_n) \neq 0$.

Proof. One implication is starightforward. Suppose the polynomials are algbraically dependent, so that $h(f_1, \ldots, f_n) = 0$ for some nonzero polynomial $h(y_1, \ldots, y_n)$. We may assume that the dgree of h is as small as possible. For each fixed j, differentiate this relation with respect to x_j we get an equation:

$$\sum_{i=1}^{n} \frac{\partial h}{\partial y_i}(f_1, \ldots, f_n) \frac{\partial f_i}{\partial x_j} = 0. \tag{8}$$

This equation for $1 \leq j \leq n$ form a system of linear equations over the field $\mathbb{C}(x_1, \ldots, x_n)$ with coefficient matrix of determinant $\mathrm{jac}(f_1, \ldots, f_n)$ and with "unknowns"

$$\frac{\partial h}{\partial y_i}(f_1, \ldots, f_n). \tag{9}$$

Because h is not constant, not all of the partial derivatives $\frac{\partial h}{\partial y_i}$ can vanish; since each has smaller degree than h, the choice of h shows that the polynomials (9) cannot all be 0. Thus the linear system has a nontrivial solution, forcing its coefficient matrix to have determinant zero.

The reverse implication is less transparent. Suppose $f_1, \ldots, f_n$ are algebraically independent. Since $\mathbb{C}(x_1, \ldots, x_n)$ has transcendence degree n over $\mathbb{C}$, the polynomials $x_i, f_1, \ldots, f_n$ are algebraically dependent for each fixed i. Let $h_i(y_0, y_1 \ldots, y_n)$ be a polynomial of minimal positive degree for which

$$h_i(x_i, f_1, \ldots, f_n) = 0.$$

Now differentiate the last equation with respect to x_k to obtain:

$$\sum_{j=1}^{n} \frac{\partial h_i}{\partial y_j}(x_i, f_1, \ldots, f_n) \frac{\partial f_j}{\partial x_k} + \frac{\partial h_i}{\partial y_0}(x_i, f_1, \ldots, f_n)\delta_{ik} = 0, \tag{10}$$

where

$$\delta_{ik} = \begin{cases} 1, & \text{if } i = k, \\ 0, & \text{if } i \neq k. \end{cases}$$

Since the f_j's are algebraically independent, h_i must have positive degree in y_0. So $\partial h_i / \partial x_i$ is nonzero and of smaller degree than h_i, forcing the value of this polynomial

at $x_i, f_1, \ldots, f_n$ to be nonzero. Transpose these terms to the right side of the equations (10) for $1 \leq i, k \leq n$, and write the equations in matrix form as

$$\Big(\frac{\partial h_i}{\partial y_j}\Big)\Big(\frac{\partial f_i}{\partial x_j}\Big) = -\Big(\delta_{ij}\frac{\partial h_i}{\partial x_j}\Big).$$

The matrix on the right side of the last equation is a diagonal matrix with nonzero determinant, so the Jacobian determinant on the left side is also nonzero. □

In the rest of this section we do **not** assume any longer that G is a reflection group.

Lemma 5. *Let r be the number of reflections in a finite matrix group $G \subset \mathrm{GL}(\mathbb{C}^n)$. Then the Laurent expansion of the Molien series about $z = 1$ begins*

$$H_G(t) = \frac{1}{|G|}(1-t)^{-n} + \frac{r}{2|G|}(1-t)^{-n+1} + O(\frac{1}{(1-t)^{n-2}}).$$

Proof. Recall from Theorem 2 the representation

$$H(t) = \frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{\det(\mathrm{Id} - \rho(g)t)}.$$

The only term $\det(\mathrm{Id} - \rho(g)t)$ in this sum to have a pole of order n at $t = 1$ is the term $\frac{1}{\det(1-t)^n}$ corresponding to the identity matrix in G. If $\frac{1}{\det(1-t)}$ has a pole of order $n-1$ at $t = 1$, then σ is a reflection and

$$\frac{1}{\det(1-\sigma t)} = \frac{1}{(1-t)^{n-1}}\frac{1}{1-\det(\sigma\cdot t)}$$

Hence the coefficient of $\frac{1}{\det(1-t)^{n-1}}$ in the Laurent expansion of $H_G(t)$ equals

$$\frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{(1-\det\sigma)},$$

where the sum ranges over all reflections σ in G. Since σ is a reflection if and only if σ^{-1} is a reflection and $\det\sigma = \det\sigma^{-1} = -1$ we conclude

$$2\sum_{\sigma\in G}\frac{1}{1-\det\sigma} = \sum_{\sigma\in G}(\frac{1}{1-\det\sigma} + \frac{1}{1-(\det\sigma)^{-1}}) = \sum_{\sigma\in G}1 = r.$$

The proof follows. □

Corollary 5 (Sum and product of the degrees)**.** *Let $G \subset \mathrm{GL}(\mathbb{C}^n)$ be a finite matrix group whose invariant ring $\mathbb{C}[x_1, \ldots, x_n]^G$ is generated by n algebraically independent homogeneous invariants $\theta_1, \ldots, \theta_n$ where $d_i = \deg\theta_i$. Let r be the number of reflections in G. Then*

$$|G| = d_1 d_2 \ldots d_n \text{ and } r = d_1 + d_2 + \cdots + d_n - n.$$

Proof. By Lemma 1, we have

$$H_G(t) = \frac{1}{1-t^{d_1}}\cdots\frac{1}{1-t^{d_n}}.$$

Multiplying $H_G(t)$ with $(1-t)^n$ and taking the Taylor expansion about $t = 1$ we find:

$$(1-t)^n H_G(t) = \frac{1}{d_1 d_2 \ldots d_n} + \frac{d_1 + d_2 + \cdots + d_n - n}{2d_1 d_2 \ldots d_n}(1-t) + O((1-t)^2).$$

Comparing with Lemma 5 completes the proof. □

Proof of Theorem 5 (only if-part). Suppose that $\mathbb{C}[x_1,\dots,x_n]^G = \mathbb{C}[\theta_1,\dots,\theta_n]$ with $\deg\theta_i = d_i$. Let H be the subgroup of generated by all reflections in G. Then by the if-part of Theorem 5, we have

$$\mathbb{C}[x_1,\dots,x_n]^H = \mathbb{C}[\psi_1,\dots,\psi_n],$$

where $\deg(\psi_j) = e_j$. Clearly $\mathbb{C}[x_1,\dots,x_n]^G \subseteq \mathbb{C}[x_1,\dots,x_n]^H$, so each θ_i is a polynomial function in the ψ's.

Since the θ's and the ψ's are both algebraically independent, the Jacobian determinant $\det(\frac{\partial\theta_i}{\partial\psi_j})_{i,j}$ is nonzero. Hence there exists a permutation π with

$$\frac{\partial\theta_{\pi(1)}}{\partial\psi_1}\frac{\partial\theta_{\pi(2)}}{\partial\psi_2}\cdots\frac{\partial\theta_{\pi(n)}}{\partial\psi_n} \neq 0.$$

This means that ψ_i actually appears in $\theta_{\pi(i)} = \theta_{\pi(i)}(\psi_1,\dots,\psi_n)$, and consequently $e_i = \deg\psi_i \leq d_{\pi(i)} = \deg\theta_{\pi(i)}$. Let r be the number of reflections in G and therefore in H. By Corollary 5, we have

$$r = \sum_{i=1}^{n}(d_i - 1) = \sum_{i=1}^{n}(d_{\pi(i)} - 1) = \sum_{i=1}^{n}(e_i - 1).$$

Since $e_i \leq d_{\pi(i)}$, we have $e_i = d_{\pi(i)}$, so again by Corollary 5 we have $|G| = d_1d_2\dots d_n = e_1e_2\dots e_n = |H|$, and hence $H = G$. □

7. LECTURE 7 (More on invariants of reflection groups).

Proposition 5. *Suppose G is a reflection group. Suppose also that $f_1,\dots,f_n$ are homogeneous G-invariants, having respective degrees $e_1,\dots,e_n$. If $f_1,\dots,f_n$ are algebraically independent and $\prod_{i=1}^n e_i = |W|$ then they form a set of basic invariants, i.e., $\mathbb{C}[W]^G = \mathbb{C}[f_1,\dots,f_n]$.*

Proof. We may assume that $e_1 \leq e_2 \leq \cdots \leq e_n$. Let $h_1,\dots,h_n$ be a set of basic invariants, of degrees $d_1 \leq d_2 \leq \cdots \leq d_n$. Since f_1 is a polynomial in the h_i's, it is clear that $e_1 \geq d_1$. We claim that this inequality holds for each i. Otherwise, let k be the first index for which $e_k < d_k$. Then each of $f_1,\dots,f_{k-1}$ must be a polynomial in $h_1,\dots,h_{k-1}$. But the field of rational functions generated by $f_1,\dots,f_k$ has transcendence degree k over $\mathbb{C}$, so cannot be contained in a field of smaller transcendence degree. This proves our claim.

Thanks to Corollary 5 and the hypothesis, $\prod_{i=1}^n d_i = |G| = \prod_{i=1}^n e_i$ forcing $d_i = e_i$ for all i. In turn, we see that the dimension of the space of homogeneous invariants of degree d generated by the f_i's agrees with that of the space generated by the h_i's, for every d. Thus, the f_i are a set of basic invariants for G. □

We are going to discuss now the **classification of complex reflection groups**. A complex reflection group is a product of so-called **irreducible** reflection groups. So, we will only discuss irreducible reflection groups in this lecture notes.

Definition 10. A complex reflection group $G \leq \mathrm{GL}(W)$ is called **reducible** if the vector space W is a reducible, G-module, i.e. it has notrivial G-submodules. If this is not the case, then G is said to be an **irreducible** complex reflection group.

The irreducible complex reflection groups were classified by **G. Shephard** and **J. Todd** in 1954. They proved that every irreducible reflection group either belongs to an infinite family $G(m,p,n)$ depending on 3 positive integer parameters (with p dividing m) or is one of 34 exceptional cases, which they numbered from 4 to 37.

Let us first introduce the notion of **monomial matrix**: by monomial matrix we mean $n \times n$ matrix such that in each row and column of the matrix there is exactly one non-zero element. If the non-zero entries of a monomial matrix are equal to 1, then the matrix is called a **permutation matrix**.

Definition 11. For any $m,p,n \geq 1$ such that $p|m$ define $G(m,p,n)$ to be the group of $n \times n$ monomial matrices with non-zero entries a_i such that the a_i are m-th roots of unity and $\prod_{i=1}^{n} a_i$ is an m/p-th root of unity.

Theorem 6. *If* $\dim W = n \geq 2$ *and if* $G \leq \mathrm{GL}(W)$ *is an irreducible complex reflection group then* G *is conjugate to* $G(m,p,n)$*, i.e., there exists* $g \in \mathrm{GL}(W)$ *such that* $gGg^{-1} = G(m,p,n)$ *for some* $m,p \in \mathbb{N}$ *and* $p|m$*.*

Note that the group $G(1,1,n)$ is isomorphic to the symmetric group S_n. Moreover, $G(1,1,n)$ acts on $\mathbb{C}^n$ by permuting coordinates.

Exercise 6. *Let* $D_n(m)$ *be the set of diagonal complex matrices with diagonal entries in the group* μ_m *of all* m*-th roots of unity. Let* $p|m$ *and* $d = m/p$*. The* d*-th power of the determinant defines a surjective morphism*

$$det^d : D_n(m) \to \mu_p.$$

Let $A(m,p,n)$ *be the kernel of the above morphism. In particular we have* $|A(m,p,n)| = m^n/p$*. Identifying the symmetric group* S_n *with the usual* $n \times n$ *permutation matrices, please, show that*

$$G(m,p,n) = A(m,p,n) \rtimes S_n.$$

Remark 7. One can show that the group $G(m,p,n)$ is irreducible if and only if $(m,p,n) \neq (2,2,2)$ and $m > 1$. Note that $G(2,2,2)$ is isomorphic to the so-called Klein group of order 4 that is isomorphic to $\mu_2 \times \mu_2$. If $m = 1$, then $G(1,p,n)$ is a subgroup of index p of the symmetric group $S_n = G(1,1,n)$.

Example 15. (i) Recall that $\mathrm{SL}_n(\mathbb{C}) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A = 1\}$. Define

$$T_n = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & & \dots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \in \mathrm{SL}_n(\mathbb{C}) \mid a_{ij} = 0,\ i \neq j \right\} = \{\mathrm{diag}(t_1,\dots,t_n) \mid t_1 \dots t_n = 1\},$$

where $\mathrm{diag}(t_1,\dots,t_n)$ is the diagonal matrix with entries t_i. One can show that T_n is isomorphic to $(\mathbb{C}^*)^{n-1}$. Denote by $N(T_n)$ the normalizer of T_n in $\mathrm{SL}_n(\mathbb{C})$, i.e., $N(T_n) = \{g \in \mathrm{SL}_n(\mathbb{C}) \mid gT_n = T_n g\}$. One can prove that

$$N(T_n) = \cup_A \{AT_n \mid A \text{ is a permutation matrix}\}.$$

We define the **Weyl group** of $\mathrm{SL}_n(\mathbb{C})$ to be the quotient $N(T_n)/T_n$ which is isomorphic to S_n. Moreover, the action of $N(T_n)/T_n$ on T_n induces the action on the n-dimensional vector space of all diagonal matrices $\{\mathrm{diag}(t_1,\dots,t_n) \mid t_1,\dots,t_n \in \mathbb{C}\}$ which is the same as the action of $G(1,1,n)$ on $W=\mathbb{C}^n$.

(ii) Consider $\mathrm{SO}_{2n}(\mathbb{C}) = \{A \in \mathrm{GL}_{2n}(\mathbb{C}) \mid A^t J_{2n} A = J_{2n},\ \det A = 1\}$, where by A^t we denote the transpose matrix of A and

$$J_k = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 0 \\ & \dots & \dots & \dots & & 0 \\ 0 & 1 & \dots & & 0 & 0 \\ 1 & 0 & \dots & & 0 & 0 \end{pmatrix}$$

is the reversed identity matrix of size $k \times k$. One can see that the group

$$T^{\mathrm{SO}}_{2n} = \left\{\mathrm{diag}(t_1,\dots,t_n,t_n^{-1},\dots,t_1^{-1}) \mid t_1,\dots,t_n \in \mathbb{C}^*\right\}$$

is a subgroup of $\mathrm{SO}_{2n}(\mathbb{C})$ isomorphic to $(\mathbb{C}^*)^n$. Analogously as above we define the Weyl group of $\mathrm{SO}_{2n}(\mathbb{C})$ to be the quotient $N(T^{\mathrm{SO}}_{2n})/T^{\mathrm{SO}}_{2n}$, where $N(T^{\mathrm{SO}}_{2n})$ is the normalizer of T^{SO}_{2n} in $\mathrm{SO}_{2n}(\mathbb{C})$. The quotient group $N(T^{\mathrm{SO}}_{2n})/T^{\mathrm{SO}}_{2n}$ acts on T^{SO}_{2n} and hence, $N(T^{\mathrm{SO}}_{2n})/T^{\mathrm{SO}}_{2n}$ induces the action on the tangent space $T_E T^{\mathrm{SO}}_{2n}$ at the identity element E of the group T^{SO}_{2n}. Moreover, $T_E(T^{\mathrm{SO}}_{2n})$ is isomorphic to the vector space $\mathbb{C}^n$ and the action of $N(T^{\mathrm{SO}}_{2n})/T^{\mathrm{SO}}_{2n}$ on $T_E(T^{\mathrm{SO}}_{2n}) \simeq \mathbb{C}^n$ is isomorphic to the action of $G(2,2,n)$ on $\mathbb{C}^n$.

(iii) Analogously as above, consider $\mathrm{SO}_{2n+1}(\mathbb{C}) = \{A \in \mathrm{GL}_{2n+1}(\mathbb{C}) \mid A^t J_{2n+1} A = J_{2n+1},\ \det A = 1\}$. One can find out that the group

$$T^{\mathrm{SO}}_{2n+1} = \left\{\mathrm{diag}(t_1,\dots,t_n,1,t_n^{-1},\dots,t_1^{-1}) \mid t_1,\dots,t_n \in \mathbb{C}^*\right\}.$$

is the subgroup of $\mathrm{SO}_{2n+1}(\mathbb{C})$ that is isomorphic to $(\mathbb{C}^*)^n$. We define the Weyl group of $\mathrm{SO}_{2n+1}(\mathbb{C})$ to be the quotient $N(T^{\mathrm{SO}}_{2n+1})/T^{\mathrm{SO}}_{2n+1}$, where $N(T^{\mathrm{SO}}_{2n+1})$ is the normalizer of T^{SO}_{2n+1} in $\mathrm{SO}_{2n+1}(\mathbb{C})$. The quotient group $N(T^{\mathrm{SO}}_{2n+1})/T^{\mathrm{SO}}_{2n+1}$ acts on T^{SO}_{2n+1} and hence, $N(T^{\mathrm{SO}}_{2n+1})/T^{\mathrm{SO}}_{2n+1}$ induces the action on the tangent space $T_E(N(T^{\mathrm{SO}}_{2n+1})/T^{\mathrm{SO}}_{2n+1})$ at the identity element E of the group T^{SO}_{2n+1}. Moreover, $T_E(T^{\mathrm{SO}}_{2n+1})$ is isomorphic to the vector space $\mathbb{C}^n$ and the action of $N(T^{\mathrm{SO}}_{2n+1})/T^{\mathrm{SO}}_{2n+1}$ on $T_E(T^{\mathrm{SO}}_{2n+1}) \simeq \mathbb{C}^n$ is isomorphic to the action of $G(2,1,n)$ on $\mathbb{C}^n$.

Matrix groups $\mathrm{SL}_n(\mathbb{C})$, and $\mathrm{SO}_n(\mathbb{C})$ play a very important role in the theory of algebraic groups (we will introduce this notion later). The Weyl groups of these groups play a very important role as well. Hence, groups $G(1,1,n)$, $G(2,1,n)$ and $G(2,2,n)$ are of great interest. In the next lecture we will compute the invariant rings of groups $G(1,1,n)$, $G(2,1,n)$, $G(2,2,n)$ and alternating group $A_n \subset S_n = G(1,1,n)$.

8. **LECTURE 8 (Invariants of some Refelction Groups).**

Consider first the symmetric group $G = S_n$. Define

$$h_i = x_1^i + \dots + x_n^i \ \ (1 \le i \le n).$$

The product of degrees of the h_i is $n! = |G|$, so to show that $\mathbb{C}[x_1, \ldots, x_n]^G = \mathbb{C}[h_1, \ldots, h_n]$, it just has to be checked (thanks to Proposition 5) that the h_i's are algebraically independent. We are going to do this using Jacobian criterion (see Proposition 4). For $1 \leq i, j \leq n$,

$$\frac{\partial h_i}{\partial x_j} = i x_j^{i-1}.$$

Thus, $\mathrm{jac}(h_1, \ldots, h_n)$ is $n!$ times the $n \times n$ the so-called Vandermonde determinant

$$D = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ & & \ldots & \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}. \tag{11}$$

Now D is well-known to equal

$$\prod_{1 \leq i,j \leq n} (x_j - x_i).$$

Hence,

$$\mathrm{jac}(h_1, \ldots, h_n) = n! \prod_{1 \leq i,j \leq n} (x_j - x_i) \neq 0$$

For G of type B_n the reasoning is similar. Here G acts on $x_1, \ldots, x_n$ by permutations and sign changes, leaving invariant

$$h_i = x_1^{2i} + \cdots + x_n^{2i} \ \ (1 \leq i \leq n),$$

whose degrees have product $2^n n! = |G|$. A quick computation yields

$$\begin{aligned} \mathrm{jac}(h_1, \ldots, h_n) &= 2^n n! \begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_1^3 & x_2^3 & \ldots & x_n^3 \\ & & \ldots & \\ x_1^{2n-1} & x_2^{2n-1} & \ldots & x_n^{2n-1} \end{vmatrix} \\ &= 2^n n! x_1 \ldots x_n \prod_{1 \leq i,j \leq n} (x_j^2 - x_i^2) \neq 0. \end{aligned}$$

The group G of type D_n acts on $x_1, \ldots, x_n$ by permutations and by changes of an even number of signs, so we can easily find invariants by modifying the preceding choice slightly:

$$h_i = \sum_{j=1}^{n} x_j^{2i} \ \ (1 \leq i \leq n-1), \ h_n = x_1 \ldots x_n.$$

The product of the degrees is $2^{n-1} n! = |G|$. With somewhat more effort than before, one finds

$$\mathrm{jac}(h_1, \ldots, h_n) = \begin{vmatrix} 2x_1 & 2x_2 & \ldots & 2x_n \\ 4x_1^3 & 4x_2^3 & \ldots & 4x_n^3 \\ & & \ldots & \\ (2n-2)x_1^{2n-3} & (2n-2)x_2^{2n-3} & \ldots & (2n-2)x_n^{2n-3} \\ \hat{x}_1 x_2 \ldots x_n & x_1 \hat{x}_2 \ldots x_n & \ldots & x_1 x_2 \ldots \hat{x}_n \end{vmatrix},$$

where $x_1 \dots \hat{x}_i \dots x_n = x_1 \dots x_{i-1} x_{i+1} \dots x_n$. Hence, one can show that $\mathrm{jac}(h_1, \dots, h_n) = (-2)^{n-1}(n-1)! \prod_{1 \le i,j \le n} (x_j^2 - x_i^2) \neq 0$.

Invariants of alternating group. Let $A_n \subset S_n$ be the alternating group that acts on $W = \mathbb{C}^n$. We claim that

$$\mathbb{C}[x_1, \dots, x_n]^{A_n} = \{f \mid f(x_{\delta(1)}, \dots) = f(x_1, ...) \text{ for all } \delta \in A_n\} = \mathbb{C}[\sigma_1, \dots, \sigma_n, D], \tag{12}$$

where $\sigma_1, \dots, \sigma_n$ are symmetric polynomials (see Example 5 from lecture notes) and $\delta = \prod_{i<j}(x_i - x_j)$ is the Vandermond determinant.

Let us first show that any $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]^{A_n}$ splits into a sum of symmetric and so-called alternating polynomial, i.e., such polynomial f that

$$\delta \cdot f = -f$$

for any $\delta \in S_n$ of odd length. Indeed, define $h(x_1, x_2, x_3, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n) = (1,2) \cdot f(x_1, x_2, x_3, \dots, x_n)$. Then

$$f + h \text{ is symmetric and } f - h \text{ is alternative.}$$

The first assertion follows from the fact that

$$\delta \cdot (f + h) = \delta \cdot f + \delta \cdot h = \delta \cdot f + \delta(1,2) \cdot f = \delta \cdot f + (1,2)\delta' \cdot f,$$

where $\delta' \in S_n$ has the same sign as $\delta \in S_n$ (please, show this! Note that any transposition can be written as a product of any other transposition and some even permutation). The second one follows because for any δ of odd length

$$\delta \cdot (f - h) = \delta \cdot f - \delta(1,2) \cdot f = \delta \cdot f - f$$

since $\delta(1,2)$ has even length and moreover

$$\delta \cdot f - f = (1,2)(1,2)\delta \cdot f - f = (1,2)f - f = h - f$$

as $(1,2)\delta \in S_n$ has even length. Therefore,

$$f = \frac{1}{2}(f + h) + \frac{1}{2}(f - h)$$

is a sum of a symmetric polynomial and an alternating polynomial.

We now claim that D divides any alternating polynomial. Indeed, for alternating polynomial f,

$$f(x_2, x_1, x_3, \dots, x_n) = -f(x_1, x_2, x_3, \dots, x_n)$$

and so $f(x_1, x_1, x_3, \dots, x_n) = 0$. Therefore, f is divisible by $x_1 - x_2$. Likewise it is divisible by all $x_i - x_j$ and hence, since $\mathbb{C}[x_1, x_2, \dots, x_n]$ is a unique factorization domain, f is also divisible by $\prod_{i<j}(x_i - x_j)$. Therefore, the ideal generated by invariants of positive degree from $\mathbb{C}[x_1, \dots, x_n]^{A_n}$ coincides with the ideal generated by symmetric functions $\sigma_1, \dots, \sigma_n$ and D. Finally, by Remark 6 we get (12).

Remark 8. By Theorem 5 and (12) we have that A_n is not a reflection group.

9. LECTURE 9 (More about Algebraic Geometry: Affine Varieties).

We have seen in Lecture 4 that every closed subset $X \subset W = \mathbb{C}^n$ is equipped with an algebra of $\mathbb{C}$-valued functions, namely the coordinate ring $\mathbb{C}[X]$. We first remark that $\mathbb{C}[X]$ determines the topology of X. In fact, define for every ideal $\mathfrak{a} \subset \mathbb{C}[X]$ the zero set in X by

$$\mathcal{V}_X(\mathfrak{a}) := \{x \in X \mid f(x) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

Clearly, we have $\mathcal{V}_X(\mathfrak{a}) = \mathcal{V}(\tilde{\mathfrak{a}}) \cap X$, where $\tilde{\mathfrak{a}} \subset \mathbb{C}[W]$ is an ideal which maps surjectively onto $\mathfrak{a}$ under the restriction map. This shows that the sets $\mathcal{V}_X(\mathfrak{a})$ are the closed sets of the topology on X induced by the Zariski topology of W. Moreover, the coordinate ring $\mathbb{C}[X]$ also determines the points of X since they are in one-to-one correspondence with the maximal ideals of $\mathbb{C}[X]$:

$$x \in X \mapsto \mathfrak{m}_x := \ker \mathrm{ev}_x \subset \mathbb{C}[X],$$

where $\mathrm{ev}_x \colon \mathbb{C}[X] \to \mathbb{C}$ is the evaluation map $f \mapsto f(x)$. This leads to the following definition of an affine variety.

Definition 12. A set Z together with a $\mathbb{C}$-algebra $\mathbb{C}[Z]$ of $\mathbb{C}$-valued functions on Z is called an affine variety if there is a closed subset $X \subset \mathbb{C}^n$ for some n and a bijection $\varphi \colon Z \xrightarrow{\sim} X$ which identifies $\mathbb{C}[X]$ with $\mathbb{C}[Z]$, i.e., $\varphi^* \colon \mathbb{C}[X] \xrightarrow{\sim} \mathbb{C}[Z]$ given by $f \mapsto f \circ \varphi$, is an isomorphism.

The functions from $\mathbb{C}[Z]$ are called regular, and the algebra $\mathbb{C}[Z]$ is called coordinate ring of Z or algebra of regular functions on Z. The affine variety Z has a natural topology, also called Zariski topology, the closed sets being the zero sets

$$\mathcal{V}_Z(\mathfrak{a}) = \{z \in Z \mid f(z) = 0 \text{ for all } f \in \mathfrak{a}\},$$

where $\mathfrak{a}$ runs through the ideals of $\mathbb{C}[Z]$. It follows from what we said above that the bijection $\rho \colon Z \xrightarrow{\sim} X$ is a homeomorphism with respect to the Zariski topology.

Clearly, every closed subset $X \subset W = \mathbb{C}^n$ together with its coordinate ring $\mathbb{C}[X]$ is an affine variety. More generally, if X is an affine variety and $Y \subset X$ a closed subset, then Y together with the restrictions $\mathbb{C}[Y] = \{f|_Y \mid f \in \mathbb{C}[X]\}$ is an affine variety, called a **closed subvariety**.

Example 16. As in Example 5, let S_n denote the symmetric group on $\{1, \ldots, n\}$ and consider the natural representation of S_n on $V = \mathbb{C}^n$ given by $\sigma \cdot e_i = e_{\sigma(i)}$, or, equivalently

$$\sigma \cdot (x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

We say that $x = (x_1, x_2, \ldots, x_n) \sim y = (y_1, y_2, \ldots, y_n)$ if and only if there exists some $\sigma \in S_n$ such that $\sigma \cdot (x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$. We claim that the orbit space $\mathbb{C}^n/\sim$ is an affine variety.

We define $\mathbb{C}[\mathbb{C}^n/\sim] = \mathbb{C}[\mathbb{C}^n]^{S_n}$ to be the symmetric polynomials in n variables and claim that $\mathbb{C}^n/\sim$ is an affine variety. To see this consider the map

$$\varphi \colon (\mathbb{C}^n/\sim) \to \mathbb{C}^n,\ x = (x_1, \ldots, x_n) \mapsto (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)),$$

where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric polynomials (see Example 5). It is easy to see that φ is surjective and that $\varphi(x) = \varphi(y)$ if and only if $x \sim y$. Thus, φ defines

a bijection $\phi\colon \mathbb{C}^n/\sim \xrightarrow{\sim} \mathbb{C}^n$, and the pull-back of the regular functions on $\mathbb{C}^n$ are the symmetric polynomials: $\phi^*\colon \mathbb{C}[x_1,\dots,x_n] \xrightarrow{\sim} \mathbb{C}[\sigma_1,\dots,\sigma_n]$.

We will need the following corollary from Nullstellensatz (see Theorem 3) in order to prove the next proposition.

Corollary 6 (from Theorem 3)**.** *The map $X \mapsto I(X)$ defines a inclusion-reversing bijection*

$$\{X \subset W \text{ closed }\} \xrightarrow{\sim} \{\mathfrak{a} \subset \mathbb{C}[W] \text{ perfect ideal}\}$$

whose inverse map is given by $\mathfrak{a} \mapsto \mathcal{V}(\mathfrak{a})$. Moreover, for any finitely generated reduced $\mathbb{C}$-algebra R there is a closed subset $X \subset \mathbb{C}^n$ for some n such that $\mathbb{C}[X]$ is isomorphic to R.

Proof. The first part is clear since $\mathcal{V}(I(X)) = X$ and $I(\mathcal{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for any closed subset $X \subset W$ and any ideal $\mathfrak{a} \subset \mathbb{C}[W]$.

If R is a reduced and finitely generated $\mathbb{C}$-algebra, $R = \mathbb{C}[f_1,\dots,f_n]$, then $R \simeq \mathbb{C}[x_1,x_2,\dots,x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is the kernel of the homomorphism defined by $x_i \mapsto f_i$. Since R is reduced we have $\sqrt{\mathfrak{a}} = \mathfrak{a}$ (see Exercise 3) and so $\mathbb{C}[\mathcal{V}(\mathfrak{a})] \simeq \mathbb{C}[x_1,x_2,\dots,x_n]/\mathfrak{a} \simeq R$. □

We start with a reduced and finitely generated $\mathbb{C}$-algebra R. Denote by $\operatorname{Spec} R$ the set of maximal ideals of R:

$$\operatorname{Spec} R = \{\mathfrak{m} \mid \mathfrak{m} \subset R \text{ a maximal ideal}\}.$$

We know from Hilbert's Nullstellensatz (see Exercise 4) that $R/\mathfrak{m} = \mathbb{C}$ for all maximal ideals $\mathfrak{m} \in \operatorname{Spec} R$. This allows to identify the elements from R with $\mathbb{C}$-valued functions on $\operatorname{Spec} R$: for $f \in R$ and $\mathfrak{m} \in \operatorname{Spec} R$ we define

$$f(\mathfrak{m}) = f + \mathfrak{m} \in R/\mathfrak{m} = \mathbb{C}.$$

Proposition 6. *Let R be a reduced and finitely generated $\mathbb{C}$-algebra. Then the set of maximal ideals $\operatorname{Spec} R$ together with the algebra R considered as functions on $\operatorname{Spec} R$ is an affine variety.*

Proof. We have already seen earlier that every such algebra R is isomorphic to the coordinate ring of a closed subset $X \subset \mathbb{C}^n$. The claim then follows by using the bijection $X \xrightarrow{\sim} \operatorname{Spec} \mathbb{C}[X]$, $x \mapsto \mathfrak{m}_x = \ker \operatorname{ev}_x$, and remarking that for $f \in \mathbb{C}[X]$ and $x \in X$ we have $f(x) = \operatorname{ev}_x(f) = f + m_x$, by definition. □

Exercise 7. *Denote by C_n the n-tuples of complex numbers up to sign, i.e., $C_n := \mathbb{C}^n/\sim$ where $(x_1,\dots,x_n) \sim (y_1,\dots,y_n)$ if $x_i = \pm y_i$ for all i. Then every polynomial in $\mathbb{C}[x_1^2, x_2^2, \dots, x_n^2]$ is a well-defined function on C_n. Show that C_n together with these functions is an affine variety. (**Hint:** Consider the map:*

$$\mathbb{C}^n \to \mathbb{C}^n,\ (a_1,\dots,a_n) \mapsto (a_1^2,\dots,a_n^2)$$

and proceed like in Example 16.)

Example 17. (1) We claim that $\mathrm{O}_n(\mathbb{C}) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid AA^t = A^tA = E\}$ is a closed subset of $\mathrm{M}_n(\mathbb{C})$ which would show that $\mathrm{O}_n(\mathbb{C})$ is an affine variety. Indeed, it is not difficult to see that

$$\mathrm{O}_n(\mathbb{C}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & & \dots & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \in \mathrm{M}_n(\mathbb{C}) \mid \sum_{\nu=1}^{n} a_{i\nu}a_{j\nu} - \delta_{ij} = 0 \mid 1 \leq i \leq j \leq n) \right\}$$

which shows the claim.

$(1)'$ Let us show that $\mathrm{SO}_n(\mathbb{C}) = \{A \in \mathrm{O}_n(\mathbb{C}) \mid \det A = 1\}$ is an affine variety. As we have shown in (1), $\mathrm{O}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ is closed. Moreover, by Example 9(1) we know that $\mathrm{SL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ is closed too. It is easy to see that $\mathrm{SO}_n(\mathbb{C}) = \mathrm{O}_n(\mathbb{C}) \cap \mathrm{SL}_n(\mathbb{C})$. Since intersection of two closed subsets $\mathrm{O}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ is closed in $\mathrm{M}_n(\mathbb{C})$ we conclude that $\mathrm{SO}_n(\mathbb{C}) \subset \mathrm{M}_n(\mathbb{C})$ is closed in Zariski topology.

(2) Let us show that $\mathrm{GL}_n(\mathbb{C})$ is an affine variety. Consider first the subset S of $n^2 + 1$-dimensional vector space

$$\mathbb{C} \times \mathrm{M}_n(\mathbb{C}) = \{(t, A) \mid t \in \mathbb{C}, A \in \mathrm{M}_n(\mathbb{C})\}$$

defined in the following way:

$$S = \{(t, A) \in \mathbb{C} \times \mathrm{M}_n(\mathbb{C}) \mid t \cdot \det A = 1\}.$$

Now, consider the map $\pi\colon\ \mathrm{GL}_n(\mathbb{C}) \to S$ that sends a matrix $A \in \mathrm{GL}_n(\mathbb{C})$ to $(\frac{1}{\det A}, A)$. It is clear that π is bijective and we conclude that $\mathrm{GL}_n(\mathbb{C})$ is an affine variety. In particular, $\mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ is an affine variety.

Exercise 8. *Show that*

$$\mathrm{Sp}_{2n}(\mathbb{C}) = \{A \in \mathrm{M}_{2n}(\mathbb{C}) \mid A^t\Omega A = \Omega\}$$

is an affine variety (is closed in $\mathrm{M}_{2n}(\mathbb{C})$*), where*

$$\Omega = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}.$$

10. LECTURE 10, (Decomposition into Irreducible Components).

We start with a purely topological notion.

Definition 13. A topological space T is called irreducible if it cannot be decomposed in the form $T = A \cup B$, where $A, B \subsetneq T$ are proper closed subsets. Equivalently, every non-empty open subset is dense.

Note that an irreducible algebraic variety is always connected but the converse is not true.

Example 18. Take $X = \{(x, y) \in \mathbb{C}^2 \mid xy = 0\}$. Here the open sets, $Y_1 = \{(x, 0) \in X \mid x \neq 0\}$ and $Y_2 = \{(0, y) \in X \mid y \neq 0\}$ do not intersect each other. And $X = \{(x, 0)\} \cup \{(0, y)\}$, where both the sets $\{(x, 0)\}$ and $\{(0, y)\}$ are connected (being homeomorphic to $\mathbb{C}$) and they intersect each other, hence the union is connected.

10.1. **Product of irreducible varieties.**

Proposition 7. *The product $X \times Y$ of two affine varieties together with the algebra*

$$\mathbb{C}[X \times Y] = \mathbb{C}[f \cdot h \mid f \in \mathbb{C}[X], h \in \mathbb{C}[Y]]$$

of $\mathbb{C}$-valued functions is an affine variety. Moreover, the canonical homomorphism

$$\mathbb{C}[X] \otimes \mathbb{C}[Y] \to \mathbb{C}[X \times Y], f \otimes h \mapsto f \cdot h,$$

is an isomorphism.

Proof. Let $X \subset \mathbb{C}^n$ and $Y \subset \mathbb{C}^m$ be closed subvarieties. Then $X \times Y \subset \mathbb{C}^{n+m}$ is closed, namely equal to the zero set $\mathcal{V}(I(X) \cup I(Y))$. So it remains to show that $\mathbb{C}[X \times Y] = \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_m]/I(X \times Y)$ is generated by the products $f \cdot h$ and that $f \cdot h \in \mathbb{C}[X \times Y]$ for $f \in \mathbb{C}[X]$ and $h \in \mathbb{C}[Y]$. But this is clear since $\bar{x}_i = x_i|_{X \times Y} = x_i|_X \cdot 1$ and $\bar{y}_j = y_j|_{X \times Y} = 1 \cdot y_j|_Y$, and $f|_X \cdot h|_Y = (fh)|_{X \times Y}$ for $f \in \mathbb{C}[x_1, \ldots, x_n]$ and $h \in \mathbb{C}[y_1, \ldots, y_m]$.

For the last claim, we only have to show that the map $\mathbb{C}[X] \otimes \mathbb{C}[Y] \to \mathbb{C}[X \times Y]$, $f \otimes h \mapsto f \cdot h$, is injective. For this, let $\{f_i \mid i \in I\}$ be a basis of $\mathbb{C}[Y]$. Then every element $s \in \mathbb{C}[X] \otimes \mathbb{C}[Y]$ can be uniquely written as a finite sum $\sum_{\text{finite}} s_i(x) f_i(y)$. If s is in the kernel of the map, then $\sum s_i(x) f_i(y) = 0$ for all $(x, y) \in X \times Y$ and so, for every fixed $x \in X$, $\sum s_i(x) f_i$ is the zero function on Y . This implies that $s_i(x) = 0$ for all $x \in X$ and so $s_i = 0$ for all i. Thus, $s = 0$ proving the claim.

Proposition 8. *A product $X \times Y$ of irreducible varieties is irreducible.*

Proof. Suppose that $Z_1, Z_2 \subset X \times Y$ are subvarieties with $Z_1 \cup Z_2 = X \times Y$. We assume that $Z_2 \neq X \times Y$ and use this to show that $Z_1 = X \times Y$. For each $x \in X$, identify the subvariety $\{x\} \times Y$ with Y . This irreducible variety is the union of two subvarieties,

$$\{x\} \times Y = ((\{x\} \times Y) \cap Z_1) \cup ((\{x\} \times Y) \cap Z_2),$$

and so one of these must equal $\{x\} \times Y$. In particular, we must either have $\{x\} \times Y \subset Z_1$ or else $\{x\} \times Y \subset Z_2$. If we define

$$X_1 = \{x \in X \mid \{x\} \times Y \subset Z_1\}, \text{ and}$$
$$X_2 = \{x \in X \mid \{x\} \times Y \subset Z_2\},$$

then we have just shown that $X = X_1 \cup X_2$. Since $Z_2 \neq X \times Y$, we have $X_2 \neq X$. We claim that both X_1 and X_2 are subvarieties of X. Then the irreducibility of X implies that $X = X_1$ and thus $X \times Y = Z_1$. We will show that X_1 is a subvariety of X. For $y \in Y$, set

$$X_y = \{x \in X \mid (x, y) \in Z_1\}.$$

Since $X_y \times \{y\} = (X \times \{y\}) \cap Z_1$, we see that X_y is a subvariety of X. But we have

$$X_1 = \bigcap_{y \in Y} X_y,$$

which shows that X_1 is a subvariety of X. An identical argument for X_2 completes the proof. □

Corollary 7. *If $X = \cup_i X_i$ and $Y = \cup_j Y_j$ are the irreducible decompositions of X and Y, then $X \times Y = \cup_{i,j} X_i \times Y_j$ is the irreducible decomposition of the product.*

10.2. **Irreducible decomposition.**

Proposition 9. *An affine variety X is irreducible if and only if its ideal $I(X)$ is prime.*

Proof. Let X be an affine variety and set $\mathfrak{a} = I(X)$. First suppose that X is irreducible. Let $f, g \notin \mathfrak{a}$. Then neither f nor g vanishes identically on X. Thus $Y = X \cap \mathcal{V}(f)$ and $Z = X \cap \mathcal{V}(z)$ are proper subvarieties of X. Since X is irreducible, $Y \cup Z = X \cap \mathcal{V}(fg)$ is also a proper subvariety of X, and thus $fg \notin \mathfrak{a}$.

Suppose now that X is reducible. Then $X = Y \cup Z$ is the union of proper subvarieties Y, Z of X. Since $Y \subsetneq X$ is a subvariety, we have $I(X) \subsetneq I(Y)$. Let $f \in I(Y) \setminus I(X)$, a polynomial which vanishes on Y but not on X. Similarly, let $g \in I(Z) \setminus I(X)$ be a polynomial which vanishes on Z but not on X. Since $X = Y \cup Z$, fg vanishes on X and therfore lies in $\mathfrak{a} = I(X)$. This shows that $\mathfrak{a}$ is not prime. □

A general variety is a finite union of "components" where a component means a maximal irreducible subset.

Theorem 7. *Any affine variety is a finite union of irreducible subvarieties.*

Proof. An affine variety X either is irreducible or else we have $X = Y \cup Z$, with both Y and Z proper subvarieties of X. We may similarly decompose whichever of Y and Z are reducible, and continue this process, stopping only when all subvarieties obtained are irreducible. A priori, this process could continue indefinitely. We argue that it must stop after a finite number of steps.

If this process never stops, then X must contain an infinite chain of subvarieties, each one properly contained in the previous one,

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \dots.$$

Their ideals form an infinite increasing chain of ideals in $\mathbb{C}[x_1, \dots, x_n]$, The union I of these ideals is again an ideal. Note that no ideal $I(X_m)$ is equal to I. By the Hilbert Basis Theorem, I is finitely generated, and thus there is some integer m for which $I(X_m)$ contains these generators. But then $I = I(X_m)$, a contradiction. □

Remark 9. Note that it is not difficult to prove that an affine variety X has a unique irreducible decomposition as a finite union of irreducible subvarieties

$$X = X_1 \cup \dots \cup X_m.$$

We call these distinguished subvarieties X_i the irreducible components of X.

Example 19. The group $\mathrm{O}_2 = \{A \in \mathrm{M}_2(\mathbb{C}) \mid AA^t = A^tA = E\}$, where E is the identity matrix has two irreducible components, namely $\mathrm{SO}_2(\mathbb{C}) := \mathrm{O}_2(\mathbb{C}) \cap \mathrm{SL}_2(\mathbb{C})$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \mathrm{SO}_2(\mathbb{C})$, and the two components are disjoint.

In fact, the condition $AA^t = E$ for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ implies that $\begin{pmatrix} a \\ b \end{pmatrix} = \pm \begin{pmatrix} d \\ -c \end{pmatrix}$.

Since $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2$ we see that $\mathrm{SO}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 = 1 \right\}$ is irreducible as well as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \mathrm{SO}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \mid a^2 + b^2 = 1 \right\}$ and the claim follows.

11. LECTURE 11, Morphisms and Constructible Sets.

11.1. Morphisms, images, preimages and fibers.

Definition 14. Let X, Y be affine varieties. A map $\varphi\colon X \to Y$ is called **regular morphism** if the pull-back of a regular function on Y is regular on X:

$$f \circ \varphi \in \mathbb{C}[X] \text{ for all } f \in \mathbb{C}[Y].$$

Thus, we obtain a homomorphism $\varphi^*\colon \mathbb{C}[Y] \to \mathbb{C}[X]$ of $\mathbb{C}$-algebras given by $\varphi^*(f) = f \circ \varphi$, which is called **comorphism** of φ. A morphism φ is called an **isomorphism** if φ is bijective and the inverse map φ^{-1} is also a morphism. If, in addition, $Y = X$, then φ is called an **automorphism**.

Definition 15. A morphism $\varphi\colon X \to Y$ is called a **closed immersion** if $\varphi(X) \subset Y$ is closed and the induced map $X \to \varphi(X)$ is an isomorphism.

Proposition 10. *A morphism $\varphi\colon X \to Y$ is a closed immersion if and only if the comorphism $\varphi^*\colon \mathbb{C}[Y] \to \mathbb{C}[X]$ is surjective.*

Proof. If φ is a closed immersion, then $\mathbb{C}[X] \simeq \mathbb{C}[\varphi(X)]$ and the regular functions on $\varphi(X)$ are restrictions from regular functions on Y, hence φ^* is surjective.

Now assume that φ^* is surjective, and put $\mathfrak{a} = \ker \varphi^*$. This is a radical ideal and so $\mathfrak{a} = I(Z)$ where $Z = \mathcal{V}_X(\mathfrak{a})$. By definition, φ^* has the decomposition $\mathbb{C}[Y] \twoheadrightarrow \mathbb{C}[Z] \xrightarrow{\sim} \mathbb{C}[X]$, i.e. φ induces an isomorphism $X \xrightarrow{\sim} Z \subset Y$. □

Exercise 9. *Let $\varphi\colon X \to Y$ and $\psi\colon Y \to Z$ be morphisms, and assume that the composition $\psi \circ \varphi$ is a closed immersion. Then φ is a closed immersion.*

11.2. Dimension.

Let A be a finitely generated $\mathbb{C}$-algebra. A set $a_1, a_2, \ldots, a_n \in A$ of elements from A are called **algebraically independent** over $\mathbb{C}$ if they do not satisfy a non-trivial polynomial equation $F(a_1, a_2, \ldots, a_n) = 0$, where $F \in \mathbb{C}[x_1, \ldots, x_n]$. Equivalently, the canonical homomorphism of $\mathbb{C}$-algebras $\mathbb{C}[x_1, \ldots, x_n] \to A$ defined by $x_i \mapsto a_i$ is injective. In order to define the **dimension of a variety** we will need the concept of transcendence degree $\operatorname{tdeg}_{\mathbb{C}} K$ of a field extension $K/\mathbb{C}$. It is defined to be the maximal number of algebraically independent elements in K. Such a set is called a **transcendence basis**, and all such bases have the same number of elements.

Definition 16. Let X be an irreducible affine variety and $\mathbb{C}(X)$ its field of rational functions. Then the **dimension** of X is defined by

$$\dim X = \operatorname{tdeg}_{\mathbb{C}} \mathbb{C}(X).$$

If X is reducible and $X = \cup_i X_i$ the irreducible decomposition, then

$$\dim X = \max_i \dim X_i.$$

Lemma 6. *Let X, Y be irreducible varieties of dimensions m, n respectively, then* $\dim X \times Y = m + n$.

Proof. It suffices to consider the case where X and Y are irreducible, see Corollary 7. Then $\mathbb{C}[X] \otimes \mathbb{C}[Y]$ is a domain as well as $\mathbb{C}(X) \otimes \mathbb{C}(Y)$. Now $\mathbb{C}(X)$ is finite over a subfield

$\mathbb{C}(x_1, \ldots, x_n)$ where $n = \dim X$, and $\mathbb{C}(Y)$ is finite over a subfield $\mathbb{C}(y_1, \ldots, y_m)$, where $m = \dim Y$. Hence, $\mathbb{C}(X) \otimes \mathbb{C}(Y)$ is finitely generated over $\mathbb{C}(x_1, \ldots, x_n) \otimes \mathbb{C}(y_1, \ldots, y_m)$. Since $\mathbb{C}(X \times Y)$ is the field of fractions of $\mathbb{C}(X) \otimes \mathbb{C}(Y)$, it follows that it is finite over $\mathbb{C}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ which is the field of fractions of $\mathbb{C}(x_1, \ldots, x_n) \otimes \mathbb{C}(y_1, \ldots, y_m)$. This completes the proof. □

Proposition 11. *Let X be an irreducible variety and let Y be a proper subvariety of X. Then $\dim Y < \dim X$.*

Proof. We can assume that Y is irreducible. If $h_1, \ldots, h_m \in \mathbb{C}[Y]$ are algebraically independent where $m = \dim Y$, and $h_i = \tilde{h}_i|_Y$ for $\tilde{h}_1, \ldots, \tilde{h}_m \in \mathbb{C}[X]$, then $\tilde{h}_1, \ldots, \tilde{h}_m$ are algebraically independent, too, and so $\dim X \geq \dim Y$. If $\dim Y = \dim X$, then every $f \in \mathbb{C}[X]$ is algebraic over $\mathbb{C}(\tilde{h}_1, \ldots, \tilde{h}_m)$. Choose $f \in \mathbb{C}[X]$ in the kernel of the restriction map, i.e. $f|_Y = 0$. Then f satisfies an equation of the form

$$f^k + p_1 f^{k-1} + \cdots + p_{k-1} f + p_k = 0,$$

where $p_j \in \mathbb{C}(\tilde{h}_1, \ldots, \tilde{h}_m)$ and k is minimal. Multiplying this equation with a suitable $q \in \mathbb{C}[\tilde{h}_1, \ldots, \tilde{h}_m]$ we can assume that $p_j \in \mathbb{C}[\tilde{h}_1, \ldots, \tilde{h}_m]$. But this implies that $p_k|_Y = 0$. Thus, since functions $\tilde{h}_1, \ldots, \tilde{h}_m$ are algebraically independent and their restrictions to Y are algebraically independent, we conclude that $p_k = 0$ and we end up with a contradiction that k is minimal. □

11.3. **Constructable sets.** Let $\varphi\colon X \to Y$ be the morphism. We ask the question if the image of open (closed) subset of X is open (closed) in Y? The answer turns to be "NO".

Example 20 (the image is not open nor closed)**.** Let $\varphi\colon \mathbb{C}^2 \to \mathbb{C}^2$, $(x, y) \mapsto (x, xy)$ be the morphism. The image of this morphism is $\mathbb{C}^2 \setminus \{(0, c) \mid c \neq 0\}$, which is not open in $\mathbb{C}^2$ but does have $\mathbb{C}^2$ as its closure. Moreover, $\mathbb{C}^2 \setminus \{(0, c) \mid c \neq 0\}$ is also not closed in $\mathbb{C}^2$. Further, the image of $\mathbb{C}^2$ is not **locally closed set**, i.e., it is not the intersection of a closed and an open subsets.

However, we will see that the image is always a so-called constructible set.

Definition 17. A subset S of an affine variety X is called **constructible** if it is a finite union of locally closed subsets.

Exercise 10. (1) *Finite unions, finite intersections and complements of constructible sets are again constructible.*

(2) *If a subset S of an affine variety X is constructible, then S contains a set U which is open and dense in $\bar{S}$.*

We present the next important result without proof.

Theorem 8 (Chevalley's Theorem)**.** *If $\varphi\colon X \to Y$ is a morphism of affine varieties, then the image of a constructible subset is constructible.*

In the next lecture we will start to study algebraic groups.

12. LECTURE 12, Algebraic Groups.

12.1. Algebraic Groups.

Definition 18. An **affine algebraic group** is an affine variety G equipped with the structure of a group, such that the multiplication map

$$\mu\colon G\times G\to G,\ (g,h)\mapsto gh^{-1}$$

is a morphism of varieties.

In this notes instead of using the slogan "affine algebraic group" we will simply use "algebraic group".

Remark 10. Let G be an algebraic group. Consider the morphism

$$\varphi_h\colon G\to G,\ \ g\mapsto hg.$$

The morphism φ_h is an isomorphism as $\varphi_{h^{-1}}$ is the inverse morphism to φ_h. Hence, φ_h maps open and closed subsets of G to open respectively closed subsets of G.

It is clear from the definition that a closed subgroup of an algebraic group is an algebraic group. Moreover, we have the following lemma.

Lemma 7. *Let U and V be dense open subsets of G. Then $G=U\cdot V$.*

Proof. Let $x\in G$. Then $x\cdot V^{-1}$ and U are dense open subsets of G. So they have to meet, forcing $x\in U\cdot V$. □

Lemma 8. *Let $H<G$ be a subgroup of an algebraic group G. Then*
(i) if H is constructible, then H coincides with its closure $\bar{H}$.
(ii) if H contains a dense open subset of its closure $\bar{H}$, then $H=\bar{H}$.
(iii) if H is locally closed, then it is closed.

Proof. $(i),(ii)$: if H is constructible, it contains a dense open subset U of $\bar{H}$, see Exercise 10(2). Then H is also open in $\bar{H}$, as H is a union $\cup_{h\in H}h\cdot U$ of open sets $h\cdot U$. By Lemma 7, $\bar{H}=H\cdot H=H$.
(iii) follows from (ii). □

Remark 11. The assertion (iii) of the lemma above is not true in the case of topological groups. For those who are familiar with topological groups, take the following example: a line with irrational slope in $\mathbb{R}^2$, gives an embedding of R into $\mathbb{R}^2/\mathbb{Z}^2$ as an everywhere dense subgroup of the torus $\mathbb{R}^2/\mathbb{Z}^2$.

Example 21. (1) Any finite group is an algebraic group. Indeed, it is easy to see that a finite set is an affine variety with discrete topology.

(2) As we have seen in Example 9, $\mathrm{SL}_n(\mathbb{C})$ is an affine variety. Moreover, one can show that the map

$$\mathrm{SL}_n(\mathbb{C})\times\mathrm{SL}_n(\mathbb{C})\to\mathrm{SL}_n(\mathbb{C}),\ (g,h)\mapsto gh^{-1}$$

is a morphism of affine varieties. Hence, $\mathrm{SL}_n(\mathbb{C})$ is an algebraic group.

(3) By Example 17 we have that $\mathrm{O}_n(\mathbb{C})$ and $\mathrm{SO}_n(\mathbb{C})$ are affine varieties. Analogously as in the case of $\mathrm{SL}_n(\mathbb{C})$ we can show that $\mathrm{O}_n(\mathbb{C})$ and $\mathrm{SO}_n(\mathbb{C})$ are algebraic groups.

(4) The group of upper triangular unipotent matrices

$$U_n = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ & & \dots & \\ 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

with 1's along the diagonal and any elements over the diagonal is an algebraic group.

(5)The group of diagonal matrices

$$T_n = \left\{ \begin{pmatrix} * & 0 & \dots & 0 \\ 0 & * & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & * \end{pmatrix} \right\}$$

with nonzero elements along the diagonal is an algebraic group. Its coordinate ring is isomorphic to $\mathbb{C}[t_1, t_1^{-1}, \dots, t_n, t_n^{-1}]$.

Lemma 9. *Let $\varphi\colon X \to Y$ be a morphism. If X is irreducible, then the closure $\overline{\varphi(X)}$ of $\varphi(X) \subset Y$ is irreducible.*

Proof. Let $Z = \overline{\varphi(X)}$. Suppose that $Z = Z_1 \cup Z_2$, where Z_1 and Z_2 are closed subsets in Y. Then $X = \varphi^{-1}(Z) = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$. Since φ is a morphism, $\varphi^{-1}(Z_1)$ and $\varphi^{-1}(Z_2)$ are closed subsets of X. Therefore, by the irreducibility of X, either $X = \varphi^{-1}(Z_1)$ or $X = \varphi^{-1}(Z_2)$. Without loss of generality, assume that $X = \varphi^{-1}(Z_1)$. Then $\varphi(X) \subset Z_1$, so $\varphi(X) \subset \overline{Z_1} = Z_1$, and $\overline{\varphi(X)} = Z_1$. Therefore, $\overline{\varphi(X)}$ is irreducible. □

Proposition 12. *Connected algebraic group is irreducible.*

Proof. One needs to prove that there is a unique irreducible component of G passing through $\{e\}$, the identity of the group G. Let $X_1, \dots, X_m$ be all irreducible components of G passing through $\{e\}$. Look at the mapping $\phi\colon X_1 \times \dots X_m \to G$, given by multiplication. Since X_i's are irreducible, so is their product and also the closure of the image of the product in G under the map ϕ (see Lemma 9). Clearly the closure of the image contains the identity and therefore the closure of the image of the map ϕ is contained in an irreducible component of G, say X_1. Since all X_i contain identity, this implies that all X_i are contained in a fixed X_1. □

Proposition 13. *The irreducible component of G passing through $\{e\}$ is a closed normal subgroup of G of finite index.*

Proof. We denote the irreducible component of G passing through $\{e\}$ by G°. Obviously, G° is closed in G. To prove that G° is a subgroup of G, we must show that whenever $x, y \in G^\circ$, $xy^{-1} \in G^\circ$. Clearly $x^{-1}G^\circ$ is also maximal irreducible subset (follows from Remark 10) and $e \in x^{-1}G^\circ \cap G^\circ$, thus $x^{-1}G^\circ = G^\circ$, i.e., $x^{-1}y \in G^\circ$ $\forall x, y \in G^\circ$. Similarly one can prove that G° is normal. An algebraic variety has finitely many irreducible components (see Theorem 7), hence G° is of finite index in G. This completes the proof. □

Remark 12. For an algebraic group G, any closed subgroup of finite index contains G°. Indeed, let H be a subgroup of G of finite index. Then H° is closed subgroup of H

of finite index which in turn is a closed subgroup of G of finite index too. Hence H° is a closed subgroup of G of finite index. Moreover, since H° is connected, $H^\circ \subset G^\circ$ is a closed subgroup of finite index. If $H^\circ \subset G^\circ$ is a proper subset, then $\dim H^\circ < \dim G^\circ$ (see Proposition 11) which means that the index of H° in G° is infinite. Therefore, $H^\circ = G^\circ$ which proves the claim.

12.2. **Some Generalities about Closures in the Zariski Topology.** Given $A \subset X$, where X is an algebraic variety, one can define A to be the smallest closed algebraic subvariety of X containing A, i.e.,

$$\overline{A} = \{Y \mid A \subset Y,\ Y \text{ is closed in } X\}.$$

In particular, if G an algebraic group and H is an abstract subgroup of G, one can talk about $\overline{H}$ which is a closed subvariety of G.

Lemma 10. *If H is an abstract subgroup of G, then $\overline{H}$ is a closed algebraic subgroup of G.*

Proof. We need to prove that $\overline{H} \cdot \overline{H} \subset \overline{H}$ and $\overline{H}^{-1} \subset \overline{H}$. Clearly, $H \subset h^{-1} \cdot \overline{H}$ for any $h \in H$ and $h^{-1} \cdot \overline{H}$ is closed in G. Hence, $\overline{H} \subset h^{-1}\overline{H}$

$$\begin{aligned}
&\Rightarrow h \cdot \overline{H} \subset \overline{H} \ \ \forall h \in H \\
&\Rightarrow H \cdot \overline{H} \subset \overline{H} \\
&\Rightarrow H \cdot \overline{h} \subset \overline{H} \ \ \forall \overline{h} \in H \\
&\Rightarrow \overline{H \cdot \overline{h}} = \overline{H} \cdot \overline{h} \subset \overline{H} \ \ \forall \overline{h} \in H \\
&\Rightarrow \overline{H} \cdot \overline{H} \subset \overline{H}.
\end{aligned}$$

Similarly by noting that the map $x \mapsto x^{-1}$ is a homeomorphism of G, one can prove that H is closed under inversion. Thus, H is a closed subgroup of the algebraic group G □

This group $\overline{H}$ is called the algebraic hull of H.

Proposition 14. *If $G \subset \mathrm{GL}_n(\mathbb{C})$ is a subgroup such that for some $d \geq 1$, $g^d = E \ \ \forall g \in G$, then G is finite.*

Proof. If G is not finite, look at $\overline{G}$, an algebraic subgroup of $\mathrm{GL}_n(\mathbb{C})$, for which $x^d = E$ continues to hold. There exists a subgroup of $\overline{G}$ of finite index, $\overline{G}^\circ$, such that $\overline{G}^\circ$ is connected. A connected algebraic subgroup $\overline{G}^\circ$, is of positive dimension, and then x^d can not be identically E (one can easily conclude it from Remark 13). Contradiction. □

Remark 13. One can show that any affine algebraic group contains a copy of $\mathbb{C}^*$ or $\mathbb{C}^+$.

Exercise 11. *Let G be a connected algebraic group. Prove that any finite normal subgroup H lies in the center of G.*

Exercise 12. *Let $\varphi\colon G \to H$ be a morphism of algebraic groups which is an isomorphism of abstract groups. Then φ is an isomorphism of algebraic groups.*

13. LECTURE 13, Actions of Algebraic Groups.

Definition 19. A G-variety is an affine variety X equipped with an action of the algebraic group G,

$$\alpha\colon G\times X\to X,\ (g,x)\mapsto g\cdot x$$

which is also a morphism of varieties. We then say that α is an algebraic G-action. Any algebraic action $\alpha\colon G\times X\to X$ yields an action of G on the coordinate ring $\mathbb{C}[X]$, via

$$(g\cdot f)(x)=f(g^{-1}\cdot x)$$

for all $g\in G, f\in\mathbb{C}[X]$ and $x\in X$. This action is clearly linear.

Lemma 11. *With the preceding notation, the complex vector space $\mathbb{C}[X]$ is a sum of finite dimensional G-stable subspaces on which G acts algebraically.*

Proof. The action morphism $\alpha\colon G\times X\to X$ yields an algebra homomorphism (see Definition 14)

$$\tilde{\alpha}\colon\mathbb{C}[X]\to\mathbb{C}[G\times X],\ f\mapsto((g,x)\mapsto f(g\cdot x)).$$

Since $\mathbb{C}[G\times X]=\mathbb{C}[G]\otimes\mathbb{C}[X]$ (see Proposition 7), we may write

$$f(g\cdot x)=\sum_{i=1}^{n}\varphi_i(g)\psi_i(x),$$

where $\varphi_1,\dots,\varphi_n\in\mathbb{C}[G]$ and $\psi_1,\dots,\psi_n\in\mathbb{C}[X]$. Then

$$g\cdot f=\sum_{i=1}^{n}\varphi_i(g^{-1})\psi_i$$

and hence the translates $\{g\cdot f\mid g\in G\}$ span a finite-dimensional subspace $V\subset\sum_{i=1}^{n}\mathbb{C}\psi_i\subset\mathbb{C}[X]$. Clearly, V is G-stable. Moreover, we have $h\cdot(g\cdot f)=\sum_{i=1}^{n}\varphi_i(g^{-1}h^{-1})\psi_i$ for any $g,h\in G$, and the functions $h\mapsto\varphi_i(g^{-1}h^{-1})$ are all regular. Thus, the G-action on V is algebraic □

This result motivates the following.

Definition 20. A **rational G-module** is a complex vector space W (possibly of infinite dimension) equipped with a linear action of G, such that every $v\in W$ is contained in a finite-dimensional G-stable subspace on which G acts **algebraically**, i.e.,

$$G\times W\to W,\ \ (g,w)\mapsto g\cdot w$$

is a morphism of affine varieties.

Examples of rational G-modules include coordinate rings of G-varieties, by Lemma 11. Also, note that the finite-dimensional G-modules are in one-to-one correspondence with the homomorphisms of algebraic groups $f\colon G\to\mathrm{GL}_n(\mathbb{C})$ for some n, i.e., with the finite-dimensional algebraic representations of G.

Some linear actions of an algebraic group G do not yield rational G-modules; for example, the G-action on $\mathbb{C}[G]$ via left multiplication, if G is irreducible and non-trivial. However, we shall only encounter rational G-modules in these notes, and just

call them G-**modules** for simplicity. Likewise, the actions of algebraic groups under consideration will be assumed to be algebraic as well.

Example 22. Let $G = \mathbb{C}^*$; then

$$\mathbb{C}[G] = \mathbb{C}[t, t^{-1}] = \sum_{n=-\infty}^{\infty} \mathbb{C}t^n.$$

Given a $\mathbb{C}^*$-variety X, any $f \in \mathbb{C}[X]$ satisfies

$$(t \cdot f)(x) = f(t^{-1} \cdot x) = \sum_{n=-\infty}^{\infty} t^n f_n(x),$$

where the $f_n \in \mathbb{C}[X]$ are uniquely determined by f. In particular, $f = \sum_{n=-\infty}^{\infty} f_n$. Since $tt' \cdot f = t \cdot (t' \cdot f)$ for all $t, t' \in \mathbb{C}^*$, we obtain

$$t \cdot f_n(x) = t^n f_n(x)$$

for all $t \in \mathbb{C}^*$ and $x \in X$. This yields a decomposition

$$\mathbb{C}[X] = \oplus_{n=-\infty}^{\infty} \mathbb{C}[X]_n,$$

where each $t \in \mathbb{C}^*$ acts on $\mathbb{C}[X]_n$ via multiplication by t^n. It follows that the product in $\mathbb{C}[X]$ satisfies

$$\mathbb{C}[X]_m \mathbb{C}[X]_n \subset \mathbb{C}[X]_{m+n}$$

for all m, n.

Definition 21. Given two G-varieties X, Y, a morphism of varieties $f\colon X \to Y$ is called **equivariant** if it satisfies $f(g \cdot x) = g \cdot f(x)$ for all $g \in G$ and $x \in X$. We then say that f is a G-**morphism**.

Proposition 15. *Let G be an affine algebraic group and X an affine G-variety. Then X is equivariantly isomorphic to a closed G-subvariety of a finite-dimensional G-module.*

Proof. We may choose finitely many generators $f_1, \ldots, f_n$ of the algebra $\mathbb{C}[X]$. By Lemma 11, the translates $\{g \cdot f_i \mid g \in G\}$, where $i = 1, \ldots, n$, are all contained in a finite-dimensional G-submodule $V \subset \mathbb{C}[X]$. Then V also generates the algebra $\mathbb{C}[X]$, and hence the associated evaluation map

$$\iota\colon X \to V^*, \quad x \mapsto (v \mapsto v(x))$$

is injective. To show that it is a closed immersion we note that $\mathbb{C}[X] \subset \mathbb{C}[V^*]$ because V generates $\mathbb{C}[X]$. Now it follows from Proposotion 10 that ι is the closed immersion; ι is equivariant by construction. □

Here are some fundamental properties of G-orbits and their closures.

Proposition 16. *With the preceding notation, the orbit $G \cdot x$ is a locally closed subvariety of X, Moreover, the closure $\overline{G \cdot x}$ is the union of $G \cdot x$ and of orbits of strictly smaller dimension. Any orbit of minimal dimension in $\overline{G \cdot x}$ is closed; in particular, the closure $\overline{G \cdot x}$ of $G \cdot x$ contains a closed orbit.*

Proof. Consider the orbit map

$$\alpha_x \colon G \to X, \quad g \mapsto g \cdot x.$$

Clearly, α_x is a morphism. Thus, $G \cdot x$ is a constructible subset of X, and hence contains a dense open subset $U \subset G \cdot x$ of $\overline{G \cdot x}$ (see Exercise 10(2)). Since G acts transitively on $G \cdot x$, we have that $G \cdot x = \cup_{g \in G} g \cdot U$ is open in $\overline{G \cdot x}$. The first part of the statement follows.

Since $G \cdot x$ is open in $\overline{G \cdot x}$ we have that $\overline{G \cdot x} \setminus G \cdot x$ has dimension strictly smaller than $\overline{G \cdot x}$ and since $\overline{G \cdot x}$ is a G-subvariety of X, $\overline{G \cdot x} \setminus G \cdot x$ is a union of orbits of G.

Now we will show that any orbit O of minimal dimension in $\overline{G \cdot x}$ is closed. Indeed, if O is not closed, then the closure $\overline{O} \subset \overline{G \cdot x}$ contains an orbit of dimension smaller than $\dim O$. Contradiction. □

Corollary 8. (*i*) *Let $\varphi \colon G \to H$ be a homomorphism of algebraic groups. Then the image of φ is a closed subgroup.*

(*ii*) *Any affine algebraic group is linear.*

Proof. (*i*) The image of φ is constructible. Hence, the statement follows from Lemma 8(*i*).

(*ii*) Let G be an affine algebraic group, acting on itself by left multiplication. For the corresponding action on the algebra $\mathbb{C}[G]$, we may find a finite dimensional G-submodule V which generates that algebra. The induced homomorphism $G \to \mathrm{GL}(V)$ is injective, and thus a closed immersion by (*i*). □

Remark 14. One could show that a connected linear algebraic group G of dimension one is commutative and it is isomorphic either to $\mathbb{C}^+$ or $\mathbb{C}^*$.

14. LECTURE 14, Reductive Groups and Hilbert's Theorem.

Definition 22. An element g of an algebraic group G is called **unipotent** if the closure of the group generated by g is isomorphic to the additive group $\mathbb{C}^+$. An algebraic group G is called **unipotent** if each element of G is unipotent.

Example 23. Consider the group of upper triangular matrices

$$U_n = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ & & \dots & \\ 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$

with 1's along the diagonal and any elements over the diagonal. One can check that each element of this group is unipotent (for U_2 this is trivial, please check it for U_3 and U_n for higher n). Hence, U_n is a unipotent group.

Definition 23. A linear algebraic group G is **reductive** if it does not contain any closed normal unipotent subgroup.

Example 24. (i) finite groups are reductive. This is clear because any unipotent group is infinite and hence can not be a subgroup of a finite group.

(ii) Algebraic torus $(\mathbb{C}^*)^n$ is a reductive group. Indeed, $(\mathbb{C}^*)^n$ does not contain non-trivial unipotent subgroup and hence, is reductive. To see this we will prove that $(\mathbb{C}^*)^n$ does not contain a copy of $\mathbb{C}^+$. Indeed, if $\mathbb{C}^+$ is a subgroup of $(\mathbb{C}^*)^n$, then there is a surjective homomorphism

$$\mathbb{C}[(\mathbb{C}^*)^n] \to \mathbb{C}[\mathbb{C}^+],$$

or, equivalently, we can write this surjective homomorphism as the following

$$\psi\colon \mathbb{C}[t_1, t_1^{-1}, \dots, t_n, t_n^{-1}] \to \mathbb{C}[x].$$

Since, $\mathbb{C}[t_1, t_1^{-1}, \dots, t_n, t_n^{-1}]$ is generated by invertible functions and $\mathbb{C}[x]$ does not contain an invertible function, it follows that ψ is trivial and hence, $(\mathbb{C}^*)^n$ does not contain a copy of $\mathbb{C}^+$.

(iii) The group $\mathrm{GL}_n(\mathbb{C})$ is reductive. Indeed, it is not difficult to see that $\mathrm{GL}_n(\mathbb{C})$ is a semidirect product of $\mathrm{SL}_n(\mathbb{C})$ which is normal in $\mathrm{GL}_n(\mathbb{C})$ and a subgroup

$$H = \left\{ \begin{pmatrix} c & 0 & 0 & \dots & 0 \\ 0 & c & 0 & \dots & * \\ & & & \dots & \\ 0 & 0 & & \dots & c \end{pmatrix} \mid c \in \mathbb{C}^* \right\} = \{cE_n \mid c \in \mathbb{C}^*\} \simeq \mathbb{C}^*,$$

where E_n is the identity matrix. In (ii) we proved that any homomorphism

$$\psi\colon \mathbb{C}[t, t^{-1}] \to \mathbb{C}[x]$$

is trivial, hence, any morphism from affine line $\mathbb{C}$ to punctured affine line $\mathbb{C}^*$ is a constant. Therefore, a normal unipotent subgroup U of $\mathrm{GL}_n(\mathbb{C}) = \mathrm{SL}_n(\mathbb{C}) \rtimes H$ should be a subgroup of $\mathrm{SL}_n(\mathbb{C})$ (since otherwise we cook up the morphism

$$U \subset \mathrm{GL}_n(\mathbb{C}) \to H,$$

where the map $\mathrm{GL}_n(\mathbb{C}) \to H$ is a projection onto H, which is nontrivial). As $\mathrm{SL}_n(\mathbb{C})$ is a simple algebraic group, i.e., does not contain a closed non-trivial proper normal subgroup, we conclude that U has to be trivial and hence $\mathrm{GL}_n(\mathbb{C})$ is reductive.

Remark 15. One can show that an algebraic group G is reductive if and only if G is **linearly reductive**, i.e., if every representation of G is completely reducible, i.e., if every representation of G is a direct sum of irreducible representations.

Theorem 9. *Let G be a reductive algebraic group, and X an affine G-variety. Then:*

(i) The subalgebra $\mathbb{C}[X]^G \subset \mathbb{C}[X]$ (consisting of regular G-invariant functions) is finitely generated.

(ii) Let $f_1, \dots, f_n$ be generators of the algebra $\mathbb{C}[X]^G$. Then the image of the morphism

$$X \to \mathbb{C}^n, \;\; x \mapsto (f_1(x), \dots, f_n(x))$$

is closed and independent of the choice of $f_1, \dots, f_n$. We denote the image of this morphism by $X/\!\!/G$.

(iii) Denote by $\pi = \pi_X\colon X \to X/\!\!/G$ the surjective morphism defined by (ii). Then every G-invariant morphism $f\colon X \to Y$ (i.e., morphism of affine varieties such that

$f(g \cdot x) = f(x)$ for all $x \in X$, $g \in G$), where Y is an affine variety, factors through a unique morphism $\varphi\colon X/\!\!/G \to Y$.

Proof. (i) The main ingredient is the **Reynolds operator for reductive groups**, defined as follows. For any G-module W, the invariant subspace W^G admits a unique G-stable complement W_G (see Remark 15). The Reynolds operator

$$R_W\colon W \to W^G$$

is the projection associated with the decomposition $W = W^G \oplus W_G$. If $f\colon W \to V$ is a morphism of G-modules, and $f^G\colon W^G \to V^G$ denotes the induced linear map, then clearly $R_V \circ f = f^G \circ R_W$. In particular, if f is surjective, then so is f^G.

When $W = \mathbb{C}[X]$, we set

$$R_X := R_{\mathbb{C}[X]}\colon \mathbb{C}[X] \to \mathbb{C}[X]^G.$$

Then R_X is $\mathbb{C}[X]_G$-**linear**, i.e., we have for any $a \in \mathbb{C}[X]^G$ and $b \in \mathbb{C}[X]$,

$$R_X(ab) = aR_X(b),$$

as follows by considering the morphism of G-modules $\mathbb{C}[X] \to \mathbb{C}[X]$, $b \mapsto ab$.

Consider an ideal I_G of $\mathbb{C}[X]^G$ generated by all invariants of positive degree. We claim that I_G is finitely generated. Indeed, consider the associated ideal $J = I_G\mathbb{C}[X]$ of $\mathbb{C}[X]$. Then J is G-stable, and $J^G = R_X(J) = I_G R_X(\mathbb{C}[X]) = I_G$. Since $\mathbb{C}[X]$ is Noetherian, this implies our claim.

We first prove assertion (i) in the case when X is a finite-dimensional G-module, say W. This follows (word by word) by the same trick as we did in the proof of (if-part) of Theorem 5.

In the general case, we may equivariantly embed X into a G-module$W$ (see Proposition 15); then the surjective G-homomorphism $\mathbb{C}[W] \to \mathbb{C}[X]$ induces a surjective homomorphism $\mathbb{C}[W]^G \to \mathbb{C}[X]^G$. Thus, $\mathbb{C}[X]^G$ is finitely generated; this completes the proof of (i).

(ii) Denote by φ the morphism

$$X \to \mathbb{C}^n, \quad x \mapsto (f_1(x), \dots, f_n(x))$$

defined in the theorem. The Zariski closure of the image of φ which we denote by Y is the set of all points $(a_1, \dots, a_n) \in \mathbb{C}^n$ satisfying:

$$\begin{aligned} &F(f_1, \dots, a_n) = 0 \text{ for all polynomial relations } F(f_1, \dots, f_n) = 0 \\ &\qquad\qquad \text{among the generators } f_1 \dots, f_n \in \mathbb{C}[X]^G. \end{aligned} \tag{13}$$

In the other words, Y is the zero set of the kernel $I \subset \mathbb{C}[a_1, \dots, a_n]$ of the homomorphism

$$\mathbb{C}[a_1, \dots, a_n] \to \mathbb{C}[X]^G, \quad a_i \mapsto f_i \text{ for } i = 1, \dots, n.$$

A priory, φ maps X to Y, and we would like to know that it is surjective on this set.

Starting with the point $a = (a_1, \dots, a_n) \in Y$ that is satisfying (13) we consider the homomoprhism of $\mathbb{C}[X]$-modules

$$p\colon \mathbb{C}[X] \oplus \cdots \oplus \mathbb{C}[X] \to \mathbb{C}[X] \quad (b_1, \dots, b_n) \mapsto \sum_{i=1}^{n} b_i(f_i - a_i).$$

Since each $f_i - a_i$ is G-invariant, we see that p is a homomorphism of G-representations. Also, we observe that the induced map p^G of G-invariants is not surjective: its image is the maximal ideal $\mathfrak{m}_a \subset \mathbb{C}[X]^G$ corresponding to the point $a \in Y$. Since G is reductive, this implies that p itself can not be surjective. Its image is therefore contained in some maximal ideal $\mathfrak{m} \subset \mathbb{C}[X]$. Then the intersection $\mathfrak{m} \cap \mathbb{C}[X]^G$ is a maximal ideal in $\mathbb{C}[X]^G$, and therefore, it coincides with the maximal ideal $\mathfrak{m}_a$. This shows that $a \in Y$ is the image of the point $x \in X$ corresponding to $\mathfrak{m}$.

The closed subvariety $Y = \varphi(X) \subset \mathbb{C}^n$ depends on the choice of generating invariants $f_1, \dots, f_n$. In other words, $Y = \operatorname{Spec} \mathbb{C}[a_1, \dots, a_n]/\sqrt{I}$. However, the ideal I is radical (that is, $\sqrt{I} = I$, since $\mathbb{C}[X]^G \subset \mathbb{C}[X]$ contains no nilpotent elements) and so Y is precisely the spectrum $\operatorname{Spec} \mathbb{C}[X]^G$.

(*iii*) The morphism π yields a homomorphism $p^* \colon \mathbb{C}[Y] \to \mathbb{C}[X]$ with image contained in $\mathbb{C}[X]^G$; this translates into our assertion. □

Remark 16. Note that the above map π is uniquely determined by the universal property (*iii*); it is called a categorical quotient (for affine varieties).

Remark 17. The assertion (*i*) of the previous theorem is usually called **Hilbert's Theorem** if X is a G-module.

15. LECTURE 15, Geometric Invariant Theory for Reductive Groups.

Remark 18. The map $\pi \colon X \to X/\!\!/G$ (see Theorem 9(*iii*)) is constant on orbits, i.e., if $x, y \in X$ are such that $\overline{G \cdot x} = \overline{G \cdot y}$, then $\pi(x) = \pi(y)$. Indeed, this is easy to see as π is G-equivariant (why?) and hence, $\pi(gx) = \pi(x)$ for any $g \in G$. This means that π is a constant on orbits. But since π is a morphism, $\pi^{-1}(\pi(x))$ is closed in X. Moreover, $G \cdot x \subset \pi^{-1}(\pi(x))$ which implies that $\overline{G \cdot x} \subset \pi^{-1}(\pi(x))$. The claim follows.

Theorem 10. *Let G be a reductive group that acts on affine variety X. If two orbit closures $\overline{G \cdot x}$ and $\overline{G \cdot y}$, $x, y \in X$ do not intersect, then there is an invariant $f \in \mathbb{C}[X]^G$ such that restriction of f to $\overline{G \cdot x}$ is zero and restriction of f to $\overline{G \cdot y}$ is one.*

Proof. Let $\mathfrak{a} \subset \mathbb{C}[X]$ be the ideal of functions vanishing on the closure $\overline{G \cdot x}$, and similarly, let $\mathfrak{a}' \subset \mathbb{C}[X]$ be the ideal of functions vanishing on the closure $\overline{G \cdot y}$. We consider the ideal $\mathfrak{a} + \mathfrak{a}'$ generated by $\mathfrak{a}$ and $\mathfrak{a}'$. Since $\overline{G \cdot x} \cap \overline{G \cdot y} = \emptyset$, by Hilbert's Nullstellensatz, we have $\mathfrak{a} + \mathfrak{a}' = \mathbb{C}[X]$.

The subsets $\overline{G \cdot x}, \overline{G \cdot y} \subset X$ are preserved by the action of G, and this means that the ideals $\mathfrak{a}, \mathfrak{a}' \subset \mathbb{C}[X]$ are subrepresentations of G. Then the homomorphism of $\mathbb{C}[X]$-modules

$$\mathfrak{a} \oplus \mathfrak{a}' \to \mathbb{C}[X], \quad (a, a') \mapsto a + a',$$

is also a homomorphism of G-representations. As we have seen above it is surjective, and so by linear reductivity (Remark 15) the map

$$(\mathfrak{a} \cap \mathbb{C}[X]^G) \oplus (\mathfrak{a}' \cap \mathbb{C}[X]^G) \to \mathbb{C}[X]^G,$$

is also surjective. In particular, there exist invariants $f \in \mathfrak{a} \cap \mathbb{C}[X]^G$ and $f' \in \mathfrak{a}' \cap \mathbb{C}[X]^G$ satisfying $f + f' = 1$. The function f vanishes on the orbit $\overline{G \cdot x}$ and takes the value 1 on the orbit $\overline{G \cdot y}$, so we are done. □

We can conclude that the algebraic quotient $X/\!\!/G$ is an affine variety (see Theorem 9) that is the set of G-orbits of X modulo the relation by which we identify two orbits of X whenever their orbit closures have non-empty intersection (follows from Theorem 10 and Remark 18). Moreover, $\mathbb{C}[X/\!\!/G] = \mathbb{C}[X]^G$. If all orbits are closed (e.g., if G is finite) then $X/\!\!/G$ is the usual orbit space. In general the quotient $X/\!\!/G$ is in a certain way the best algebraic approximation to the orbit space X/G;

Example 25. Let $\mathbb{C}^*$ acts on $\mathbb{C}^2$ by $\lambda \cdot (x, y) = (\lambda x, \lambda y)$. The $\mathbb{C}^*$-orbits are the punctured lines $\{(\lambda x, \lambda y) \mid \lambda \in \mathbb{C}^*\}$ for $(x, y) \neq (0, 0)$ as well as the origin $\{(0, 0)\}$. The set theoretical quotient is simply the set of these orbits. However, this set of orbits does not have a structure of an affine variety. Moreover, there is the notion of a **variety** which is more general than the notion of an affine variety. And the set theoretical quotient $\mathbb{C}^2/\mathbb{C}^*$ does not have a structure of a variety.

Let us now look at orbits $\{(\lambda x, \lambda y) \mid \lambda \in \mathbb{C}^*\}$ for $(x, y) \neq (0, 0)$ and the origin $\{(0, 0)\}$ and discover which of these orbits are closed in $\mathbb{C}^2$. It is clear that the origin $\{(0, 0)\} \subset \mathbb{C}^2$ is closed (please, check it). Moreover, it is not difficult to see that punctured lines $\{(\lambda x, \lambda y) \mid \lambda \in \mathbb{C}^*\}$ are never closed in $\mathbb{C}^2$. Therefore, there is the unique closed orbit. Hence, $\mathbb{C}^2/\!\!/\mathbb{C}^*$ is a point. Alternatively, this can be seen by looking at the invariant ring $\mathbb{C}[\mathbb{C}^2]^{\mathbb{C}^*} = \mathbb{C}$ (see page 4) and we conclude that $\mathbb{C}^2/\!\!/\mathbb{C}^* = \operatorname{Spec}\mathbb{C}$ that is a point.

Example 26. Let $\mathbb{C}^*$ acts on $\mathbb{C}^2$ by $\lambda \cdot (x, y) = (\lambda x, \lambda^{-1} y)$. The $\mathbb{C}^*$-orbits are

(i) the origin $\{(0, 0)\}$;
(ii) the punctured x-axis $\{(x, 0) \mid x \in \mathbb{C}^*\}$;
(iii) the punctured y-axis $\{(0, y) \mid y \in \mathbb{C}^*\}$;
(iv) for each $c \in \mathbb{C}^*$, the conic $\{(x, y) \mid xy = c\}$.

It is not difficult to see that orbits from (iv) and (i) are closed. Moreover, the orbits from (ii) and (iii) are not closed as the closure of $\{(x, 0) \mid x \in \mathbb{C}^*\}$ is $\{(x, 0) \mid x \in \mathbb{C}\}$ and analogously the closure of $\{(0, y) \mid y \in \mathbb{C}^*\}$ is $\{(0, y) \mid y \in \mathbb{C}\}$. Hence, the closed orbits are parameterized by $\mathbb{C}$ (which is affine variety). In contrast, the set theoretical quotient $\mathbb{C}^2/\mathbb{C}^*$ is the set of all orbits that does not have a structure of an affine variety.

As we have seen in Example 4, $\mathbb{C}[\mathbb{C}^2]^{\mathbb{C}^*} = \mathbb{C}[x, y]^{\mathbb{C}^*} = \mathbb{C}[xy]$. Hence, $\mathbb{C}^2/\mathbb{C}^* = \operatorname{Spec}(\mathbb{C}[xy])$ is an affine line $\mathbb{C}$ and the quotient map is given by

$$\mathbb{C}^2 \to \mathbb{C}, \quad (x, y) \mapsto xy.$$

Exercise 13. *Consider the set* $\mathrm{M}_2(\mathbb{C})$ *of* 2×2 *matrices over* $\mathbb{C}$*, embedded in* $\mathbb{C}^4$ *by*

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} \mapsto (w, x, y, z).$$

Let $G = \mathrm{GL}(2, \mathbb{C})$ *act on* X *by conjugation. That is, for* $A \in G$, $M \in \mathrm{M}_2(\mathbb{C})$*, define* $A \cdot M = AMA^{-1}$*. Then we have* $\mathrm{M}_2(\mathbb{C})/\!\!/G = \operatorname{Spec}\mathbb{C}[w, x, y, z]^G$*. We know for matrices that the determinant and trace are invariant under conjugation. These are the polynomials* $det = wz - xy$ *and* $tr = w + z$*, so we have* $\mathbb{C}[wz - xy, w + z] \subset \mathbb{C}[w, x, y, z]^G$*. Please, show that*

$$\mathbb{C}[wz - xy, w + z] = \mathbb{C}[w, x, y, z]^G.$$

We have seen in Example 25 and Example 26 different actions of $\mathbb{C}^*$ on $\mathbb{C}^2$. The next statement classifies all $\mathbb{C}^*$-actions on $\mathbb{C}^2$.

Proposition 17. *Let $\mathbb{C}^*$ acts on $\mathbb{C}^2$. Then one can choose coordinates in $\mathbb{C}^2$ such that $t \cdot (x, y) = (t^a x, t^b y)$, where $t \in \mathbb{C}^*$, $(x, y) \in \mathbb{C}^2$ and $a, b \in \mathbb{Z}$, $|a|, |b|$ are coprime.*

Remark 19. What about classification of $\mathbb{C}^*$-actions on $\mathbb{C}^3$? This problem is very complicated and such actions where classified only in 1996 by **Kaliman, Koras, Makar-Limanov, and Russell.**

As we have already seen, if G is a reductive group, then the quotient $\mathbb{C}^n /\!\!/ G$ is an affine variety. It turns out that if $\mathbb{C}^n /\!\!/ G$ is one-dimeniosnal, i.e., if $\mathbb{C}^n /\!\!/ G$ is a curve, then such a curve is isomorphic to an affine line $\mathbb{C}$. If the quotient is 2-dimensional, then the situation becomes much more complicated.

Theorem 11 (Gurjar, Koras, and Russell, 2008)**.** *Let G be a reductive algebraic group acting algebraically on an affine space $\mathbb{C}^n$. If $X = \mathbb{C}^n /\!\!/ G$ is two-dimensional, then X is isomorphic to $\mathbb{C}^2/G$ for a finite group G (we can assume that $G \leq \mathrm{GL}(\mathbb{C}^2)$).*

We know essentially nothing about 3-dimensional quotients $\mathbb{C}^n /\!\!/ G$.

16. LECTURE 16, Unipotent Groups and their Invariants.

By Corollary 8 we know that any affine algebraic group can be embedded into some $\mathrm{GL}_n(\mathbb{C})$. Therefore, we can identify G with its image in $\mathrm{GL}_n(\mathbb{C})$. We have seen above (see Definition 22) that an element g of an algebraic group G is called **unipotent** if the closure of the group generated by g is isomorphic to the additive group $\mathbb{C}^+$. One can show that this is equivalent to the fact that g can be written as a sum $1 + n$ for some nilpotent matrix n, i.e., matrix such that n^k is a zero matrix for some natural k.

Theorem 12 (Lie-Kolchin theorem)**.** *Let G be a unipotent subgroup of $\mathrm{GL}(W)$ for some non-zero finite dimensional vector space W. Then G has a common eigenvector in W.*

Proof. Identify W with $\mathbb{C}^n$ where $n = \dim W$. We use induction on n. The result is obvious if $\dim W = 1$ (every $v \in W$ is a common eigenvector of G), so assume $\dim W > 1$. Suppose W has a proper non-zero subspace V stable under G. Then by induction hypothesis there exists a common eigenvector $v \in V \subset W$ for G.

Therefore we may assume that W is an irreducible G-module. We need the following (which we present here without proof)

Theorem of Burnside: if R is a subalgebra of the associative algebra of endomorphisms $\mathrm{End}(W)$ of a vector space W which acts irreducibly on W, then $R = \mathrm{End}(W)$.

Now, the assumption that G is unipotent implies that trace $\mathrm{Tr}(g) = \mathrm{Tr}(1) = \dim W$ for all $g \in G$ (please, check it!). Writing g as $1 + n$ with n nilpotent, we have for all $h \in G$:

$$\mathrm{Tr}(h) = \mathrm{Tr}(gh) = \mathrm{Tr}(h + nh) = \mathrm{Tr}(h) + \mathrm{Tr}(nh).$$

Therefore, $\mathrm{Tr}(nh) = 0$. Now, the $\mathbb{C}$-linear combinations of the elements of G must also satisfy this. These form a subalgebra R of $\mathrm{End}(W)$, which acts irreducibly on

W since G does. Burnside's theorem then implies that for all $h \in \mathrm{End}(W)$ and for all $g = 1 + n \in G$, $\mathrm{Tr}(nh) = 0$. Taking h to be the standard unit matrices E_{ij}, we see that we must have $n = 0$ (by E_{ij} , we mean the matrix whose (i, j)th entry is 1 and all other entries are 0). Hence $G = 1$ and since W is irreducible, $\dim W = 1$, a contradiction. □

Corollary 9. *If $G \leq \mathrm{GL}_n$ is a unipotent group, then G is conjugate to a subgroup of upper triangular matrices $U_n \subset \mathrm{GL}_n(\mathbb{C})$.*

Proof. By Theorem 12, G has a common eigenvector $v \in W = \mathbb{C}^n$. Let W_1 be a vector space generated by $\langle v \rangle$. Then G acts on W/W_1, the image of G in $\mathrm{GL}(W/W_1)$ is again unipotent. Induction on $\dim W$ then allows us to construct a basis of W with respect to which elements of G are represented by upper triangular matrices. The claim follows. □

Next we present a classical result of **B. Kostant** and **M. Rosenlicht** proved for the first time in 1961.

Theorem 13. *A unipotent group U acts on affine variety X with closed orbits, i.e., for any $x \in X$, $U \cdot x \subset X$ is a closed subset.*

Proof. Consider the orbit $O = U \cdot x$ and its closure $Y = \overline{U \cdot x}$ that is affine subvariety of X. Assume $O \neq Y$. By Proposition 16, $Z = Y \setminus O$ is a closed subset of X. Consider a nonzero polynomial $f \in \mathbb{C}[Y]$ with the property that the restriction of f to Z is a zero polynomial. Consider an irreducible U-submodule M of $\mathbb{C}[Y]$ that contains f. By Theorem 12 there exists a nonzero $g \in M^U$. In particular, since g is U-invariant, it has to be constant on O and hence constant on $\overline{O}$. As g takes the value zero on Z, it has to zero everywhere on Y. This contradicts the choice of g and proves the theorem. □

Remark 20. It is not hard to prove that the property of acting with closed orbits on affine varities characterizes unipotent groups among connected algebraic groups.

We have seen in Theorem 9 that for any reductive group G and G-module W, $\mathbb{C}[W]^G$ is finitely generated. It was not known until 1958 if a similar result holds for unipotent groups. In 1958 **Nagata** gave the following example which shows that for a unipotent group U and a certain U-module W, $\mathbb{C}[W]^U$ is not finitely generated.

Example 27 (**counter example of Nagata to Hilbert's fourteenth problem**)**.** This is the counter example of Nagata to Hilbert's fourteenth problem. Take $a_{i,j}$ algebraically independent over $\mathbb{Q}$, where $i = 1, 2, 3$ and $j = 1, 2, \ldots, 16$. Let $G \subset \mathrm{GL}(32, \mathbb{C})$ be the group of all block diagonal matrices

$$\begin{pmatrix} A_1 & & \\ & A_2 & \\ & \cdots & \\ & & A_{16} \end{pmatrix},$$

where

$$A_j = \begin{pmatrix} c_j & c_j b_j \\ 0 & c_j \end{pmatrix}$$

for $j = 1, 2, \ldots, 16$. Here the c_j and b_j are arbitrary complex numbers such that $c_1 c_2 \ldots c_{16} = 1$ and $\sum_{j=1}^{16} a_{i,j} b_j = 0$ for $i = 1, 2, 3$. Then one can prove that $\mathbb{C}[x_1, \ldots, x_{32}]^G$ is NOT finitely generated.

Remark 21 (Quotient by unipotent groups)**.** By Theorem 13 all orbits of unipotent group U that acts on an affine variety X are closed. Then one could think that $X/U = X/\!\!/U$. The problem is that $\mathbb{C}[X]^U$ is not neccesarily finitely generated. But even if $\mathbb{C}[X]^U$ is finitely generated, then X/U not necessarily coincides with $X/\!\!/U$. Actually, $X/U \subset X/\!\!/U$ is an open subset.

Remark 22. If G is a so-called **semisimple algebraic group** (i.e., product of simple algebraic groups[1]) or a unipotent group and $\mathbb{C}^n/\!\!/G$ is two-dimenisonal, then $\mathbb{C}^n/\!\!/G$ is isomorphic to an affine plane $\mathbb{C}^2$.

[1]algebraic group is called **simple** if it does not contain closed normal nontrivial subgroups

References

[Br10] Michel Brion, *Introduction to actions of algebraic groups*, Les cours du CIRM, Tome 1 (2010) no. 1, pp. 1-22.

[Ka01] Kane, Richard *Reflection Groups and Invariant Theory*, ISBN 978-1-4757-3542-0.

[Kr14] Hanspeter Kraft, *Algebraic Geometry – An Introduction*, Lecture Notes, 2014.

[KrP14] Hanspeter Kraft and Claudio Procesi, *Classical Invariant Theory – A Primer*, Lecture Notes, 1996.

[St08] Bernd Sturmfels, *Algorithms in Invariant Theory*, Lecture Notes, 2008.