

KOSTANT'S PROBLEMS 1 AND 2

VIPUL NAIK

ABSTRACT. The first of three main problems Kostant discusses in his paper is: given a k algebra S with a group G acting on it, and J being S^G , what is the structure of S over J ? Problem One: is S finitely generated as a J module? Here, I have a look at this problem and what goes into solving it. I also discuss the solution to Problem Two: When is the restriction map to an orbit an isomorphism on the space of harmonic polynomials?

1. OVERVIEW

1.1. **Content from Kostant.** In this article, I cover the following parts of Kostant's paper:

- Pages 327-330, including Propositions 0.1 and 0.2, which I call here Kostant's First Problem and Kostant's Second Problem respectively. The theorems are located at theorem 3 and theorem 4 respectively in this article.
- Section 1, Parts 1.1 - 1.3 (pages 335 -340) and Part 1.5 (342-344). These parts in the paper give detailed proofs for the first two of Kostant's problems.

I have also added more facts and tidbits picked from other places and my own explanations based on my understanding of the topic. I do *not* prove results about the harmonic polynomials (viz their orthogonality to positive degree invariant polynomials) in this article. That is in a separate piece on Bilinear Forms (file name: `bilinearform.tex`).

I have also omitted a proof of one of the results, namely Lemma 2, Section 1.2. The techniques used for that are Lie algebra theoretic rather than purely algebraic, so I shall cover that proof in a separate piece on Lie algebras (file name: `liealgebraforkostant.tex`).

1.2. **Presentation.** In this article, I talk of relations between algebras and their subalgebras. In between I also throw in a group action. Further, I keep moving between different levels of generality, with the specialization increasing as I move along the paper.

- (1) The second section gives basic definitions of finite generatedness and freeness both "module theoretically" and "algebra theoretically". It relates these questions to the questions of integral and algebraic extensions.
- (2) The third section is about freeness and generating sets. It specifically discusses how linear relations in one place give rise to linear relations in the other. This is as background for the big results that follow.
- (3) The fourth section describes the group action problem, in three levels of generality: a group acting on a commutative algebra, a group acting on an algebra of functions, and a linear group acting on the polynomial ring. The concept of invariant subring is introduced and we look at the approach of understanding the group via the relation between the ring and its invariant subring. We also provide a general *recipe* for determining the invariant subring.
- (4) The fifth section works the way through to a proof of a sufficient condition for the ring to be module theoretically free over its subring of invariants. (Kostant's first problem).
- (5) The sixth section does a little more work to provide sufficient conditions for Kostant's second problem.
- (6) The seventh section looks at some general examples of the question of module theoretic freeness, some of them being based on Kostant's results, and others using a theorem of Chevalley.

2. FINITE GENERATEDNESS AS MODULES AND ALGEBRAS

2.1. **Finitely generated modules.** Basic results about finitely generated modules over a fixed common base ring:

- A finite sum of finitely generated modules is finitely generated.

- A quotient of a finitely generated module is finitely generated.
- A submodule of a finitely generated module may not be finitely generated.
- Any algebra over the ring that is finitely generated as a module is finitely generated as an algebra with at most that many generators. The converse, however, may not be true.

A module (over a fixed ring) such that every submodule of it is finitely generated is said to be **Noetherian**_(defined). Clearly, every submodule of a Noetherian R module is also a Noetherian R module. A ring is said to be **Noetherian**_(defined) if it is Noetherian as a module over itself.

Some basic facts about Noetherian modules and ring:

- A direct sum of Noetherian modules is Noetherian, as is a quotient. Hence every finitely generated module over a Noetherian ring is a Noetherian module.
- A polynomial ring over a Noetherian ring is Noetherian.

Any module that is finitely generated over a subring is also finitely generated over the whole ring. Further, any module that is Noetherian over the subring is Noetherian over the whole ring. Now, given a module over a ring, we may want to extend it to a module over a bigger ring. This is possible through the *extension of scalars* via a tensor product. The question: what can we infer about the behaviour of the module over the original ring based on the behaviour of its extension over the extended ring? We explore a special case of this question in the next subsection.

2.2. Algebraic extensions. In general, a finite degree extension of a ring may not be a free module. Some definitions:

Definition. Our notation will be R for the base ring and S for the extension, viz an R algebra.

- S is said to be **algebraic**_(defined) over R if every element in S satisfies a polynomial in $R[x]$.
- S is said to be **algebraically finitely generated**_(defined) over R if it is finitely generated as an R algebra.
- S is said to be **integral**_(defined) over R if every element of S satisfies a monic polynomial in $R[x]$.
- S is said to be **module theoretically free**_(defined) over R if it is free as an R module.
- S is said to be **module theoretically finitely generated**_(defined) over R if it is finitely generated as an R module.
- R is said to be **large**_(defined) in S if every nontrivial ideal of S intersects R nontrivially.

Some basic facts:

- Every module theoretically finitely generated extension is algebraic. For a field, it is also algebraically finitely generated.
- Every integral extension is algebraic. Every extension that is algebraic and algebraically finitely generated is module theoretically finitely generated.
- When R is a field, then any extension of R is module theoretically free, and any algebraic extension is integral. A field is always a large subring in any extension.

Some facts which are true for arbitrary algebraic extensions of fields hold for *integral* extensions of integrally closed integral domains. A ring is said to be **normal**_(defined) or **integrally closed**_(defined) if any element in its field of fractions that is integral over it, lies in the ring itself.

Claim. An integral domain is a large subring in any algebraic extension of it.

Proof. Let R be the base ring and S be an integral extension. Let I be a nontrivial ideal in S with nonzero $x \in I$. By algebraicity of the extension, x satisfies a polynomial over R , say $p(x) = 0$. Since $x \neq 0$, and R is an integral domain, we may reduce $p(x)$ to a polynomial with nonzero constant term. Thus $0 = p(x) = xq(x) + c$. Hence, $c \in I$, and $c \in R$ because the polynomial is over R .

When p is a monic polynomial c is simply the norm of x . □

Claim. Any algebra obtained as an integral extension of finite degree over an integrally closed integral domain is free as a module over it, with the same size of generating set.

It is easy to see that if we extend scalars to the quotient field, then we have the extended module as a free module (in fact, a vector space) over the field. Thus, we can find a basis for the extended module over the field. By “clearing denominators” we can find a basis over the field for the extended module whose elements lying in the integral extension itself. Now, we use the **trace form**_(first used)

$$(x, y) \mapsto \text{Trace}(xy)$$

This form is from the extended module to the field but it takes things within the integral extension to within the field. Note: We use the fact that the extension is integral and the the base ring is integrally closed. We now look at the dual basis over the field and observe that in this dual basis, all elements within the integral extension can be expressed as linear combination with “integer” coefficients.

This result can be viewed again as follows: given any polynomial in a huge ring S containing R , the subalgebra of S generated by the roots of the polynomial is an algebra over the subalgebra generated by the coefficients of the polynomial. Moreover, this algebra extension is of finite degree, hence it is algebraically finite. The big question: is it module theoretically finitely generated? Yes, under suitable assumptions.

3. RELATING VARIOUS LINEAR DEPENDENCES

3.1. Passing to and from subalgebras. A typical question we’ll be dealing with is:

How do we relate the linear independence of elements over a smaller subalgebra to linear independence of elements over a bigger subalgebra?

Clearly, any nontrivial linear dependence in a smaller subalgebra carries over to a nontrivial linear dependence in an algebra containing it. When can we say the converse? That is, under what conditions can we guarantee that a *nontrivial* linear dependence over the bigger subalgebra gives a nontrivial linear dependence over the smaller subalgebra? Here’s a result in that direction:

Claim. Let $A \leq B \leq C$ be rings. Let $\rho : B \rightarrow A$ be a retraction (that is, a homomorphism from B to A that is identity on A). Let K be the kernel of ρ and KC be the ideal generated by K in C . Suppose M is a complement to KC as an A module in C , and M also contains A . Suppose further that C is free as a B module. Then linear independence in M over B is the same as linear independence over A .

The meaning and significance will be clearer from the proof:

Proof. First, an observation: Consider a nontrivial linear relation in M over B . Take the projection map $\tilde{\rho}$ of C on M with kernel KC . This map, when restricted to B , is the same as ρ . Under the map, there are two possibilities for a nontrivial linear relation:

- It remains nontrivial.
- All the coefficients of the linear relation are from K , and hence the relation becomes trivial.

Now we begin the proof: By assumption, C is free over B . Hence, we have a basis of C over B . Express the elements in M as linear combinations of elements from the basis of C over B . Now, any nontrivial B linear relation among these elements would mean a B linear relation among the elements in the basis, which is per force a trivial relation. Thus, there is at least one vanishing minor in a matrix describing the collection of elements of M over the basis of C . Clearly, applying $\tilde{\rho}$ to this will continue to give a zero minor, and we then have a linear dependence over A . \square

3.2. Passing to and from quotients. Another question we’ll consider is:

How do we relate linear dependence of elements over an algebra to linear dependence over quotients?

Now here’s a word of caution. Given any linear dependence of elements over an algebra, the quotient homomorphism gives a linear dependence over the quotient algebra. However, it is possible that a *nontrivial* linear dependence over the algebra gives rise to the *trivial* linear dependence over the quotient algebra.

So what do we do about this? We can do a lot of things. For one, we try to show something of the sort:

Collect a family of homomorphisms such that if an element maps to zero under each, then it is indeed zero.

We’ll come back to this later.

3.3. A preliminary result. We begin with a result that holds in the *graded* case:

Claim. Let J be a graded subalgebra of a connected graded k algebra S (k is a field). Suppose J^+ denotes the direct sum of the homogeneous components of positive degree, and J^+S is the ideal generated by J^+ . Suppose further that H is a graded complement to J^+S (and hence, in particular, H contains k). Then:

$$S = JH$$

The proof follows from a small observation: in the equation $S = J^+S + H$, replacing the S on the right hand side by JH gives $S \subseteq JH$. On its own, this observation proves nothing because all it says is $S \subseteq JH \implies S \subseteq JH$. However, the grading lets us transform the above to a proof by induction on the degree of the filtrations.

Proof. The proof follows by induction on the degree of homogeneous complements. let S^n denote the n^{th} filtration of S , that is, the sum of the graded components $S_0, S_1 \dots S_n$. Then we prove by induction on n that S^n lies inside JH .

Base case: $S^0 \subseteq H$, so $S^0 \subseteq JH$.

Induction step: Suppose $S^{(n-1)}$ lies inside H . Observe that any element of S_n can be written as $\sum_i j_i s_i + h$ where $j \in J^+$, $s \in S$ and $h \in H$. In fact, by degree considerations, we must have that each $s_i \in S^{(n-1)}$. But we know that $S^{(n-1)} \subseteq JH$. So, we obtain that S^n is also contained inside JH . \square

An aside: the gradation of S is not canonical and is not left invariant under the action of a linear automorphism. However, the *filtration* of S is invariant under all linear automorphisms. Hence the *degree* of a polynomial is invariant under linear automorphisms.

3.4. A characterization of freeness.

Theorem 1 (Characterization of module freeness). Let J be a subalgebra of the graded k algebra S . Let J^+ denote a submodule complement to k in J and J^+S be the ideal generated by J^+ . Let H be a module theoretic complement to J^+S in S , such that M contains k . Suppose further that $JH = S$.

Then the following are equivalent:

- (1) The map $J \otimes H \rightarrow S$ given by $f \otimes g \mapsto fg$ is an isomorphism.
- (2) S is free over J .
- (3) Let M be a k submodule intersecting J^+S trivially. Then linear independence within M is equivalent to linear independence over J .

Proof. A k basis of M provides an S basis of J . Hence, we have (1) \implies (2).

The proof of (3) \implies 1 runs by putting $M = B$.

The part (2) \implies (3) follows from the claim in section 3.1. The terminological dictionary is:

New notation	Notation in 3.1
k	A
J	B
S	C
J^+	K
J^+S	KC
M	M

\square

3.5. J versus J^+S . When S is a connected graded k algebra, there is an ideal complement to the base field, namely the direct sum of all the homogeneous components of positive degree. Note that this ideal is not invariant under automorphisms of the filtration. Thus, to any subring T of S , we can consider the ideal generated by T^+ (the intersection of T with the ideal of positive elements). This is what we do in the case $T = J$.

In case S is the polynomial ring in finitely many indeterminates, we have the following:

- Suppose T is the subring generated by a collection of homogeneous polynomials of positive degree. Then T^+S is the ideal generated by the same polynomials.
- In particular, if T is a free algebra in one polynomial, T^+S is a principal ideal. We know that for principal ideals, demanding that the *ideal* being prime is equivalent to demanding that the *generator* be prime. Because S is a unique factorization domain, this translates to saying that the generator must be an irreducible polynomial.

We shall return to these observations after establishing basic results of Kostant.

4. THE GROUP ACTION SETUP

4.1. Formulation of the problem. The basic problem of interest for us: “determine whether certain given naturally occurring algebra extensions are algebra theoretically or module theoretically finitely generated”. One natural source of extensions is via a *group action*.

Let S be an algebra¹ over a field k . Suppose a group G acts on S . Let $J = S^G$ be the subring of invariants. What is the nature of S as a J algebra, and as a J module? Some questions:

- Is S algebraic, algebraically finitely generated, or module theoretically finitely generated over J ?
- Does J have a natural module theoretic, ideal theoretic, or subalgebra complement in S ? What are the properties of this ideal complement?

I'll make some remarks about the finite generatedness of S over J . Consider the (noncommutative) ring JG which is basically the ring of all linear combinations in G with coefficients in J . Then, S is a JG module. When G is a finite group, the formal sum $\sum_{g \in G} g$ maps S into its invariant subring J . What we would love would be the following:

- S is free over J as a module.
- The number of generators of S over J is equal to the size of G , with the fact that for any subgroup W of G , S is free as a S^W module, which in turn is free as a J module, and the sizes of the generating sets are $|W|$ and $|G : W|$ respectively.
- There is a module theoretic complement to J in S which is the regular representation of JG (as a module).

We shall see later that a theorem of Chevalley guarantees the following for certain finite group actions. However, these conditions are too demanding for the usual actions of matrix groups on the polynomial ring. So we must settle for weaker results.

In this preliminary study, Kostant does not pay much importance to G directly and only exploits it via the proxy of its orbit structure. After discussing two main results of Kostant (Theorems 3 and 4) we shall return to these original motivations.

4.2. Determining invariant functions. The above general situation becomes more exciting in the specific case when S is an *algebra of functions*. Here, the notion of invariant function has a concrete geometric interpretation.

Let k be a field and X be any set (it could be an affine space, a projective space, a variety). Let S be a k algebra of functions $X \rightarrow k$ with addition and multiplication defined pointwise. Clearly, S contains all constant functions.

Suppose G is a group acting on X . This gives an action of G on the algebra of *all* functions from X to k . The action is $(g.s)(x) = s(g^{-1}(x))$. This means that, for $s \in S$, we calculate s , not at x , but at the point which comes to x under the action of g . If elements of S go to elements of S under this action, then we get an action of G on S .

An *invariant function* is then a function $s \in S$ such that $s = s.g^{-1}$ for every $g \in G$. This is equivalent to requiring the value of s to be constant on each orbit in X under G action. The *invariant function* notion gives a Galois correspondence between the ring S of functions and the group G , where $s \in S$ and $g \in G$ are related if and only if $g.s = s$. This is an example of a *fixed point correspondence*.

Some immediate conclusions:

- If two groups G_1 and G_2 define the same orbits on X then the ring of invariant functions is the same. Thus the closure of a group with respect to the fixed point correspondence, at the very least contains all elements that preserve orbits for this group.
- For an orbit O , let I_O be the ideal of functions in S that vanishes on O . Then the subring R_O of functions constant on O is precisely $I_O + k$ where k here denotes the ring of constant functions. The ring of invariant functions under the action of G is

$$\bigcap_O R_O = \bigcap_O (I_O + k)$$

There are thus three correspondences that Kostant works with:

- The *orbit decomposition* in X under G . Translate: What does the orbit of each point look like? What are the sets in X that arise as unions of orbits?
- The *vanishing correspondence* between S and X . Translate: What are the closed sets in X under S action and how does the topology look? What are the closed ideals with respect to the correspondence?
- The *fixed point correspondence* between G and S . Translate: Which functions in S are G invariant?

¹in this article, algebra shall always stand for commutative, associative algebra

Some terminology. Given a subgroup H of G , a k submodule of S is said to be H invariant (as a submodule) if the action of any $h \in H$ takes the submodule to itself. A little result:

Claim. Under the vanishing correspondence, the closed ideal corresponding to an H invariant subset of X is H invariant as a submodule of S . Conversely, the closed set corresponding to a H invariant ideal is H invariant as a subset of X .

4.3. The polynomial setup. Kostant discusses the above problem when S is the polynomial ring over k in n variables and G acts on S via a linear action on k^n . Thus, (assuming the action to be faithful) G is embedded as a subgroup of $GL(X) = GL_n(k)$.

The most important thing about this is that linear automorphisms of k^n give rise to automorphisms of S that preserve polynomial degree. That is, under any linear automorphism, the degree of a polynomial remains invariant.

A word of caution here. The homogeneous components of the gradation are *not* preserved under a linear automorphism. However, it does preserve the *filtration* associated with the gradation.

The scalar linear transformations on X , viz multiplication by elements of k^* , induce the following map on S : the map corresponding to an element c takes a polynomial p and returns the polynomial $x \mapsto p(x/c)$. This is a natural action of the group k^* on X . A question: which modules are k^* invariant with respect to this action? A submodule of S that is invariant under k^* action is termed a **homogeneous submodule**_(defined).

When $X = k^n$ and S is the polynomial ring, the closed sets with respect to the vanishing correspondence are called the **Zariski closed sets**_(defined) and an irreducible Zariski closed set is termed an **affine variety**_(defined).

Definition. A subset of k^n is termed a **cone**_(defined) if it is closed under the action of k^* by scalar multiplication and contains the origin. A **tip free cone**_(defined) is a cone without the origin.

Then, as a special case of the claim in the previous subsection, the Zariski closed set corresponding to a homogeneous ideal is a cone or tip free cone, and the ideal of functions vanishing on a cone is a homogeneous ideal.

4.4. Notation. We'll alternate between the general setup viz S being an algebra of functions $X \rightarrow k$, and the specific setup where S is the polynomial ring in n variables acting as functions by the evaluation map on $X = k^n$. Notation first:

Symbol	meaning
k	field
X	space
G	group acting on X
S	algebra of functions $X \rightarrow k$
O_x	orbit of $x \in X$
I_O	ideal of functions vanishing on O
R_O	subring of functions constant on O
J	G invariant functions

In the case of the polynomial ring, we have:

Symbol	meaning
k	field
X	vector space over k
G	subgroup of $GL(X)$
S	algebra of functions $X \rightarrow k$
O_x	orbit of $x \in X$
I_O	ideal of functions vanishing on O
R_O	subring of functions constant on O
J	G invariant functions

5. TOWARDS A SUFFICIENT CONDITION FOR FREENESS

5.1. Orbit restriction and linear relations. The million dollar question here is:

How does linear dependence of elements of S relate to the linear dependence of their restrictions to a particular orbit?

Restricting to an orbit is equivalent to passing to the quotient by the ideal of functions vanishing on that orbit. Thus, the above question relates to the earlier question of what happens to a linear relation upon passing to a quotient.

For an orbit O , recall that:

- The ring $I_O + k = R_O$ is the ring of functions constant over the orbit O .
- The ring J is the ring of functions constant on each orbit. So J lies inside $I_O + k$.
- The ring k is the ring of constant functions. k lies inside J . Moreover, the homomorphism sending each element of R_O to its value on the orbit is a map $R_O \rightarrow k$ such that the restriction to J maps surjectively to k . In fact, this homomorphism is a retraction.

A linear relation over J , when restricted to an orbit, gives a linear relation over k . However, a nontrivial relation may not give rise to a nontrivial relation: it could give rise to a trivial relation over the orbit O in case all the coefficients of the relation are in I_O . (We already mentioned the general version of this problem in Section 3.2).

5.2. A special situation. The notation continues: G is acting on a vector space X and has an induced action on an algebra of functions S from X to k . J is the ring of invariant polynomials.

Definition. The group action² is said to have **dense zero set property**_(defined) or **DZSP**_(defined) if the following happens. Take any linear relation in S over J . Then, the set of points $x \in X$ such that the linear relation restricted to x is trivial, is either empty or is a dense subset with respect to the vanishing correspondence (that is, its closure in the vanishing correspondence is the whole space).

Suppose the group action satisfies the DZSP. Then, we have the following result:

Claim. If the group action has DZSP, then a collection of members of S that is linearly independent when restricted to an orbit is linearly independent over J .

Proof. Suppose f_i with $1 \leq i \leq k$ is a finite collection of functions whose restrictions to an orbit O are linearly independent. Suppose the f_i themselves have a linear dependence over J . This linear relation restricts to a trivial linear relation on the orbit O . Hence, the set of points on which it restricts to a trivial linear relation is dense, by DZSP.

This means that the coefficients of the linear relation vanish on a dense subset of the space X . But then they must also vanish on the closure of this subset, and hence, the coefficients vanish over the whole of X . Thus, each coefficient is the zero function. So the linear relation is trivial. \square

5.3. The matrix of differentials.

Theorem 2 (DZSP for $k = \mathbb{C}$). In case the underlying field is the field of complex numbers, and G is a Lie group, then the set of points for which a given linear relation restricts to the trivial relation is an open set in the usual complex topology, and is hence a Zariski dense set if nonempty. Thus, DZSP holds for $k = \mathbb{C}$.

The basic ingredient of this proof is a pretty analytic function whose being nonzero characterizes linear independence. Thus, for any point where it is nonzero, there is a neighbourhood where it is nonzero as well. The proof uses the idea of the matrix of differentials. Observe that although DZSP is a purely algebraic property, the proof goes via the Euclidean and analytic route.

And now for the important result:

Corollary 1. Let $k = \mathbb{C}$ and G be a Lie group. Then, if a collection of elements of S is linearly independent over \mathbb{C} when restricted to an orbit, the collection is linearly independent over J .

5.4. Relations over the complement of J^+S . Recall that the vanishing correspondence between the set X and the algebra S is given by the relation $s(x) = 0$.

Claim. Let I be an ideal in an algebra S of functions $X \rightarrow k$ for some set X . Suppose I is closed under the vanishing correspondence, that is, I is precisely the ideal of functions that vanish on the vanishing set of I . Let P be the vanishing set of I . Suppose L is a module theoretic complement to I in S , and $L(P)$ be the restriction of L as functions on P . Then given elements in L , a nontrivial linear relation (over k) among their images in $L(P)$ gives a nontrivial linear relation among the elements themselves.

²The group plays no direct role, it only plays a proxy role by determining a subring J comprising invariant polynomials.

Proof. Let e_1, e_2, \dots, e_n be elements in L whose restrictions to P satisfy a nontrivial linear relation. Then there is a relation $\sum_{i=1}^n \lambda_i e_i(x) = 0$ valid for all $x \in P$. Let $f \in S$ be the function given as $x \mapsto \sum_{i=1}^n \lambda_i e_i(x)$. Since each $e_i \in L$, $f \in L$. But because f vanishes on the zero set of P , we also have $f \in I$. This forces f to be the zero function, giving $\sum_{i=1}^n \lambda_i e_i(x) = 0$ for all $x \in X$. \square

Corollary 2. With the same notation as in the claim above, if we assume k to be algebraically closed, it suffices, by **Hilbert’s nullstellensatz** (result assumed), to know that I is a radical ideal. That will automatically guarantee that it is closed under the vanishing correspondence.

Corollary 3. With the same notation and assumptions as in the claim above, suppose D is a dense subset of P . Then linear independence of elements of L is equivalent to linear independence of their restrictions to D .

5.5. Statement and proof. Use the standard notation: k is the field, X a k vector space, and S the polynomial ring over X . J is the invariant subring and J^+S is the ideal generated by the positive part of J , namely J^+ . Let P be the zero set of the ideal J^+S . Clearly, P is a cone.

Theorem 3 (Kostant’s First Problem for \mathbb{C}). If J^+S is a radical ideal, $k = \mathbb{C}$ and there is an element x such that O_x is dense in P in the Zariski sense, then S is free over J .

Proof. We will show the third equivalent characterization described in section 1. Namely, we’ll show that if M is a module theoretic complement to J^+S , then any collection of elements in M that is linearly independent over $k = \mathbb{C}$ is linearly independent over J .

We shall prove the contrapositive: Any nontrivial linear relation between elements of M over J gives a nontrivial linear relation over \mathbb{C} .

We combine two results already proved:

- (1) Corollary 1. This tells us that any nontrivial linear relation between elements of M over J gives a nontrivial linear relation between their restrictions to the orbit O_x , over \mathbb{C} .
- (2) Corollary 3. This tells us that any nontrivial linear relation restricted to the orbit O_x (over \mathbb{C}) extends to a nontrivial linear relation on the whole space, over \mathbb{C} .

\square

A few observations. Because J^+S is a radical ideal, and its Zariski set is the Zariski closure of the orbit of a single point, we know that J^+S is irreducible, and hence prime. So we can assume that at the outset without any loss of generality.

We shall now concern ourselves with two questions:

- What information will help us deduce that J^+S is prime? This is where *algebraic geometry*(topic name) comes in.
- Is there a *natural* choice of a complement to J^+S ?

I look at these problems in another file, viz `bilinearform.tex`.

6. QUASI REGULAR ELEMENTS

6.1. The second of Kostant’s problems. Recall the following terminology for the orbit of a point $x \in X$. When we aren’t specifically interested in the point, we’ll drop the point from the superscript or subscript.

Letter	Meaning
O_x	orbit of x under G action
G^x	stabilizer of x under G
$I(O)$	ideal of functions vanishing on O
$R(O)$	ring of functions constant on O
P_x	P intersected with closure of $\bigcup O_{cx}$
$S(O_x)$	quotient $S/I(O_x)$
$R(O_x)$	ring of all rational functions on O_x

An important focus of Kostant’s paper is to look at “nice orbits”. It should be possible to study behaviour over the whole space by looking only at a “nice orbit”. We have already seen a result which states that orbits dense inside P are “nice with respect to H in the sense that any \mathbb{C} linear dependence over H in the orbit extends to a \mathbb{C} linear dependence in the whole space.

For every point $x \in X$, there is a natural mapping $\gamma_x : H \rightarrow S(O_x)$ that sends each element of H to its quotient modulo $I(O_x)$. Since $S = JH$, and γ_x maps J to constant functions, we have that the map γ_x restricted to H is surjective.

The question:

When is the map γ_x a bijection? That is, under what circumstances is it true that knowing the restriction of an element in H to the orbit O_x suffices to determine the element of H ?

We have already given a partial answer, one which we have already seen in a different guise:

Claim. If O is a dense orbit in P , and J^+S is closed in the vanishing correspondence (viz a radical ideal in case of an algebraically closed field) then the map γ_x is a bijection.

Proof. Because J^+S is a radical ideal, we have that any function vanishing on the whole of P is in J^+S . Since O is dense in J^+S , we further obtain that any function vanishing on the whole of O is in J^+S . In particular, any function in H which vanishes on the whole of O must be zero. Thus, the kernel of γ_x is trivial and γ_x is a bijection. \square

Can we generalize this to other orbits?

Yes, but not quite. Let us assume that J^+S is a prime ideal and that there is a dense orbit O in J^+S . Then, it turns out that orbits that are dense on their own but are dense in the projectivization, are also “special orbits” in the sense that the corresponding γ map is a bijection?

Definition. A point $x \in X$ is said to be **nice**_(defined) if $P_x = P$.

Claim. The set of nice points in X is a tip free cone, that is, it is invariant under the action of k^* by scalar transformations.

Proof. The action of k^* on X by scalar multiplication corresponds to its action on the polynomial ring as follows: for multiplying X by c , replace the formal variable y by the variable y/c . This induces an automorphism on S and under that automorphism, the fact of whether or not γ_x is an isomorphism doesn't change. \square

We now work in \mathbb{C} , with *closure* meaning closure in the usual Euclidean topology. Formally, let P_x denote the intersection with P of the closure of the union of the orbits of cx where $c \in \mathbb{C}^*$. A point $x \in X$ is said to be **quasi regular**_(defined) if $P_x = P$. Then, the claim is:

Theorem 4 (Kostant's second problem). Suppose J^+S is a prime ideal and there is an orbit O dense in J^+S . Suppose further that the underlying field k is \mathbb{C} . Then the map γ_x is an isomorphism for every quasi regular point x .

Proof. The basic proof idea is this: if the set of nice points is nonempty, it contains a set open in the Euclidean topology. By the fact that $P_x = P$, any nonempty open set must intersect at least one O_{cx} . But then, cx is itself a nice point, and hence, so is x .

The fact that the set of nice points contains an open set follows from the same argument which shows the DZSP. \square

7. STEPPING BACK

7.1. The more general concern. Our original concern: “figure out how certain algebras look as extensions of certain subalgebras”. In this case, we figured out how an algebra looks over the subalgebra of fixed points under a group action. In fact, we proceeded in three steps:

- First, we just talked of the invariant subalgebra under a group action.
- Then, we specialized to the case where the algebra was the algebra of functions on a set, and the group was acting on that set.
- Then, we specialized to the case where the group was a subgroup of the group $GL(n)$ acting on the vector space k^n and the algebra was the algebra of polynomial functions.
- Finally, we fixed the ground field to be \mathbb{C} .

In the rest of the article, we explore the questions: which of the results discussed for polynomials over \mathbb{C} generalize to polynomials over any algebraically closed field, any field, or even better, to any algebra of functions. How special is the position in which Kostant's results place polynomials?

7.2. Quick examples. Recall the setup: G is a subgroup of $GL(X) = GL_n(V)$ and we study the action of G on S which is the polynomial ring on $X = k^n$. To understand this action, we determine the subring of G invariant polynomials, namely J , and then look at J^+S , the ideal generated by the elements of positive degree in J .

We then try to study S as a J module. Below, we discuss some examples. The first few examples reveal tautologies, while later examples reveal deeper subtleties.

7.2.1. *The whole of GL.* When $G = GL_n(k)$ with the usual action on k^n , then there are only two orbits: the point 0, which is a closed orbit, and the subset $k^n - \{0\}$ which is Zariski dense. Hence I_O for the second orbit is trivial, and R_O is the ring of constant functions. So J is also the ring of constant functions. Thus, we have:

- J^+S is the trivial ideal, hence it is a prime and hence also a radical ideal.
- P is the whole space, and contains a dense orbit, namely the orbit $k^n - \{0\}$.
- All points of $k^n - \{0\}$ are quasi regular.
- H is the space of all polynomials.

Notice that GL satisfies the hypotheses for Kostant's First Theorem (theorem 3). Thus, S is a free module over k . We already know that: the polynomial algebra is a countably generated free module over k , with the monomials forming a basis. We also conclude, applying the Second Theorem (theorem 4) that the restriction map of S to the nonzero orbit is an isomorphism.

Note that $SL_n(k)$ has the same orbit decomposition as $GL_n(k)$ and hence its "closure" with respect to the Galois correspondence is $GL_n(k)$.

7.2.2. *The Borel group– upper triangular matrices.* The orbits under the group $B_n(k)$ of upper triangular matrices are the subspaces with the first r coordinates being 0 and the next coordinate being nonzero, as r varying from 1 to n . Again, the orbit with $r = 0$ is Zariski dense, so we have:

- J is the ring of constant functions, J^+S is trivial. Hence it is prime and also a radical ideal.
- P is again the whole space.
- All the points in the dense orbit (viz the orbit with the first coordinate nonzero) are quasi regular. There are no other quasi regular points.

Again, the two conditions for applying Theorem 3 are satisfied. This tells us that S is free as a module over k , which we already know. Applying Theorem 4 also doesn't tell us anything new.

7.2.3. *The orthogonal group.* The group $O_n(k)$ of orthogonal matrices has orbits as the spheres centered at origin: namely the loci of $\sum_i x_i^2 - r = 0$ with r varying over k . Note first of all that all orbits are Zariski closed subsets. An easy result shows that if the orbits under a group acting on S are of the form $p(x) = c$, then the invariant subring is the subring generated by $p(x)$.

Theorem 5. If the orbits under the action of a group on the k vector space V are all of the form $p(x_1, x_2 \dots x_n) = c$ with p a fixed polynomial and c a parameter, then the invariant subring under the group action is the subring generated by the polynomial p .

Proof. Suppose $q(x)$ is a polynomial constant on each orbit $p(x) = c$. Take any nonempty orbit. Then, $q(x)$ must be a constant c_1 plus an element in the ideal generated by $p(x) - c$. That is:

$$q(x) - c_1 = q_1(x)(p(x) - c)$$

Note that both $q(x) - c_1$ and $p(x) - c$ are invariant on every orbit, and hence, so is their ratio. Thus $q_1(x)$ also lies inside the invariant subring. If, by induction on the degree, we assume that $q_1(x)$ is in the polynomial subring generated by $p(x)$ then we obtain that $q(x)$ is also in the polynomial subring. \square

As an easy corollary, the invariant subring J for the orthogonal group is the subring generated by the **sum of squares polynomial**_(defined) namely $\sum_{i=1}^n x_i^2$. A polynomial in this subring is termed a **radical polynomial**_(defined).

The ideal J^+S is the principal ideal generated by the sum of squares polynomial.

The corresponding differential operator to the sum of squares polynomial is the usual Laplacian derivative, and a polynomial invariant under this operator is termed a **harmonic polynomial**_(defined). The space of harmonic polynomials forms a natural complement to the principal ideal generated by the sum of squares polynomial.

The famous "separation of variables theorem" for orthogonal polynomials tells us that every polynomial is a finite sum of terms, each of which is a product of a radical polynomial and a harmonic polynomial. This is the special case of $S = JH$ for G being the orthogonal group.

So the facts are:

- J^+S is a principal ideal generated by the sum of squares polynomial. Is it prime? Is it radical?
- P is the set on which the sum of squares polynomial vanishes. It is a single orbit, and hence every point in it has an orbit dense in P . Moreover, it is nonempty, because $0 \in P$.
- All the points in P are quasi regular.

For two variables, J^+S is definitely *not* a prime ideal (over \mathbb{C}). What can we say for more variables? Of course, over \mathbb{R} , J^+S is a prime ideal for any number of variables greater than 1.

7.2.4. *The symplectic group.* The action of the symplectic group preserves a certain nondegenerate bilinear form. Thus, orbits under this action are subsets such that the corresponding quadratic form is the same at all points in the subset. It seems that the subring of invariants J is the generated by a single polynomial namely the polynomial ring over the corresponding quadratic form. Thus J^+S is the ideal generated by that same quadratic polynomial.

Will fill this up more later.

7.2.5. *The unitary group.* When the underlying field is \mathbb{C} , and G is the unitary group, the orbits are $\sum_i x_i \bar{x}_i - r = 0$ with r varying over nonnegative real numbers. Notice that these equations are not polynomial equations over \mathbb{C} , though they are polynomial equations over \mathbb{R} . Thus, the orbits do not appear to be Zariski closed in \mathbb{C} , though they are Zariski closed in \mathbb{R} (and hence closed in the Euclidean topology).

I will fill this up later.

7.3. The symmetric group and other finite groups.

7.3.1. *The symmetric group.* The symmetric group is about as nice a group as you can get. When $G = S_n$ the ring of invariant polynomials is the polynomial ring in certain polynomials called the elementary symmetric functions. Equivalently, it is also the subring generated by the power sum polynomials. The transformation back and forth is done via the **Newton identities** (result assumed).

Question: how does S , the ring of all polynomials, look as a ring extension of J , the ring of invariant polynomials?

First, the usual Kostant level checking:

- The ring of invariants J is the polynomial ring in the elementary symmetric polynomials.
- The ideal J^+S is the ideal generated by the elementary symmetric polynomials. A natural complement to this is the space of all polynomials that are killed by all symmetric differential operators.
- The vanishing set P of the ideal J^+S is really small – namely the origin alone. That is because all the symmetric functions on the variables are zero, forcing all variables to be 0. Thus, P is a single orbit, it contains a point whose orbit is dense, and that is the only quasi regular point.
- The space of invariant polynomials is obtained as the space of all polynomials obtained by differentiating the Vandermonde determinant. These are the so called **antisymmetric functions** (first used).

Here, J^+S is far from a prime ideal, so theorem 3 cannot be applied. In any case, the symmetric group is not a Lie group, so it doesn't satisfy the setting for satisfying DZSP.

However, we can still ask other questions related to the symmetric group in action. Firstly, observe that each x_i is integral over J , because the polynomial $\prod_i (x - x_i)$ is by definition over $J[x]$. Thus, the whole of S is an integral extension of J . Notice also that the ring J with elements $x_1, x_2 \dots x_r$ thrown in is an extension of degree $n(n-1) \dots (n-r+1)$ over J , and hence the ring S is an extension of degree $n!$ over J .

Remarkably, although we cannot apply theorem 3 in this case, we can still conclude that S is a free algebra over J , based on a theorem of Chevalley.

7.3.2. *Other finite groups.* Chevalley proved the following remarkable theorem for all finite reflection groups, which settles all the questions raised in section 4.1 positively. Namely:

Theorem 6 (Chevalley). If G is a finite group generated by reflections then $S = J \otimes H$ and the action of G on H is equivalent to the regular representation.

I will fill this up later.

INDEX

- affine variety, 6
- algebraic extension, 2
- algebraically finitely generated extension, 2
- antisymmetric functions, 11

- cone, 6

- dense zero set property, 7
- DZSP, 7

- extension
 - algebraic, 2
 - algebraically finitely generated, 2
 - integral, 2
 - module theoretically finitely generated, 2
 - module theoretically free, 2

- harmonic polynomial, 10
- Hilbert's nullstellensatz, 8
- homogeneous submodule, 6

- integral extension, 2
- integrally closed ring, 2

- large subring, 2

- module
 - Noetherian, 2
- module theoretically finitely generated extension, 2
- module theoretically free extension, 2

- Newton identities, 11
- nice point, 9
- Noetherian module, 2
- Noetherian ring, 2
- normal ring, 2

- point
 - nice, 9
 - quasi regular, 9
- polynomial
 - harmonic, 10
 - radical, 10

- quasi regular point, 9

- radical polynomial, 10
- ring
 - integrally closed, 2
 - Noetherian, 2
 - normal, 2

- submodule
 - homogeneous, 6
- subring
 - large, 2
- sum of squares polynomial, 10

- tip free cone, 6
- trace form, 2

- variety
 - affine, 6

- Zariski closed sets, 6