Annihilators of simple modules and periodic subvarieties

Jason Bell

University of Waterloo,
joint with Dragos Ghioca (Romanian)

jpbell@uwaterloo.ca

May 2019

What are primitive ideals?

A two-sided ideal P of a ring R is called *primitive* if it is the annihilator of a simple left R-module.

For example, if we take $R = M_2(\mathbb{C})$ and we take the left module M to be all column vectors $\mathbb{C}^2$, then M is a simple left R-module and we can see that the annihilator of M is zero, because if A is a 2×2 matrix such that $Av = 0$ for every $v \in M$ then $A = 0$. This means (0) is a primitive ideal of R.

Somewhat relatedly, I should mention that an ideal I of a ring R is *prime* if whenever $JL \subseteq I$ with J, L ideals of R then either J or L is contained in I. This coincides with the usual definition of a prime ideal that I assume most people are used to in the case that R is commutative.

We let $\mathrm{Spec}(R)$ denote the set of prime ideals of R. This set is a topological space with the Zariski topology.

We note that we say R is a primitive (respectively prime) ring if (0) is a primitive (resp. prime) ideal of R.

In general, primitive ideals are always prime ideals but prime ideals need not be prime. For example, in the polynomial ring $\mathbb{C}[x]$ the ideal (0) is not primitive. I'll leave that as an exercise if you haven't seen this.

Warning: I'm cheating by defining primitive ideals to be annihilators of simple left modules. Technically, these are called *left primitive* ideals and right primitive ideals can be defined analogously. George Bergman, while he was still an undergraduate, gave an example of a ring in which the zero ideal is left primitive but not right primitive.

Bergman's example, it should be noted, is somewhat strange and pathological. For most noetherian rings one encounters in practice left primitivity and right primitivity coincide, and so we shall not make any distinction.

Facts about primitive ideals

- Every ring with 1 has at least one primitive ideal.
- Primitive ideals are always prime ideals.
- In a simple ring (0) is a primitive ideal.
- In a commutative ring primitive ideals are precisely the maximal ideals.
- (Jacobson density theorem) If P is a primitive ideal of a ring R then R/P embeds "densely" in a ring of linear endomorphisms $\mathrm{End}_D(V)$ of a left D-vector space over a division D.

So why should I care about the primitive ideals of a ring R?

I'll give you two reasons.

The first reason is that one often understands a ring via its irreducible representations (i.e., the simple modules). For example, this is an important part of finite group theory with the representation theory of finite groups and many local-global principles for commutative rings can be interpreted in this framework.

This works well when dealing with finite groups but with noncommutative rings it is often an intractable problem to understand the simple modules, so Dixmier proposed that one should instead try to obtain a coarser understanding by understanding the primitive ideals (the annihilators of simple modules) instead.

So we can think of finding the primitive ideals of a ring as giving a "coarser" version of what we do when we find all the irreducible representations of a finite group. One can also hope that this information will then help us with structure theory problems about the ring.

To give a slightly better picture, a big part of Jacobson's way of studying many ring theory problems dealt with reducing problems to the primitive case.

What he'd do is that he'd try to argue that one could assume that the Jacobson radical is trivial. For rings with trivial Jacobson radical, we know something strong: R embeds in a direct product of rings of the form R/P with P a primitive ideal; then by using projections one can often reduce to just understanding the rings R/P.

Finally, he could often use the Jacobson density theory to reduce questions about R/P to linear algebra. (Admittedly, infinite-dimensional linear algebra and over division rings, but nothing's perfect ....)

The second reason is via analogy with classical algebraic geometry.

Recall that the primitive ideals in a commutative ring are precisely the maximal ideals. Algebraic geometry tell us that if k is an algebraically closed field and A is a finitely generated commutative k-algebra then the maximal ideals correspond to the points of an affine variety X in a natural way.

Just as in the commutative case, the set of prime ideals, $\mathrm{Spec}(R)$, of a ring can be endowed with a topology (the Zariski topology), and the primitive ideals form a distinguished subset of this space.

So we can think of the collection of primitive ideals (the primitive spectrum) of a ring R as being a topological space in the same way and it is often the case that interesting classes of rings have interesting primitive spectra, just as in the case with commutative rings. Also, at the very least they are isomorphism invariants.

Example

If we take the ring $\mathbb{C}\{x, y\}$ with relation $xy = 2yx$ then one can show that the primitive ideals are the zero ideal along with the ideals $(x, y - \alpha)$, $\alpha \in \mathbb{C}^*$, $(x - \beta, y)$, $\beta \in \mathbb{C}^*$, and (x, y).

If we instead used the relation $xy = yx$, we'd get the polynomial ring in two variables and the Nullstellensatz tells us that the primitive ideals correspond to points on the plane via the correspondence $(x - \alpha, y - \beta) \mapsto (\alpha, \beta)$. In our first case we are just getting the points $(0, \alpha)$ and $(\beta, 0)$, i.e., the x- and y-axes, along with a "dense" point (0).

So hopefully I've convinced you that understanding the primitive ideals is worthwhile. The next question is: How do we identify the primitive ideals?

We know the primitive ideals are all prime ideals, so the question becomes understanding which elements of $\mathrm{Spec}(R)$, the prime ideals of R, are primitive.

The Dixmier-Moeglin equivalence

The Dixmier-Moeglin equivalence is a result (obviously due to Dixmier and Moeglin), which characterizes the primitive ideals in $\mathrm{Spec}(R)$ when R is the enveloping algebra of a finite-dimensional complex Lie algebra. It gives two equivalent conditions to being primitive, one topological and one algebraic.

Theorem: (Dixmier-Moeglin) Let R be the enveloping algebra of a finite-dimensional complex Lie algebra. Then for a prime ideal P of R the following are equivalent:

- P is primitive;
- $\{P\}$ is locally closed in $\mathrm{Spec}(R)$;
- P is *rational*.

What is locally closed?

You might know what it means for a set in a topological space to be locally closed: it just means that it's an intersection of a closed set and an open set. Well, $\mathrm{Spec}(R)$ is a topological space with the Zariski topology so for $\{P\}$ to be locally closed it means that the set of all primes properly containing P has to be closed.

In practice, this just means that there is some element $a \in R \setminus P$ such that a is in *every* prime ideal that properly contains P. For example, in the ring $\mathbb{C}\{x, y\}$ with relation $xy = 2yx$ you can check that every prime ideal properly containing (0) contains the element xy.

What is rational?

Rational is a bit more fun. We all know that a commutative domain has a field of fractions. As it turns out, there is a more general fact due to Alfred Goldie:

If S is a prime noetherian ring then S has a "noncommutative field of fractions," $\mathrm{Frac}(S)$, which we obtain by inverting the non-zero divisors in R. This ring is obviously not a field but it is the next best thing: it's a simple Artinian ring, so it is isomorphic to $M_n(D)$ for some $n \geq 1$ and some division ring D.

If R is a algebra over the complex numbers then we say that P is rational if $\mathrm{Frac}(R/P)$ has centre equal to the complex numbers (the base field of R).

For the rest of this talk, $k = \mathbb{C}$, and R will be a finitely generated associative (but not necessarily commutative) noetherian k-algebra. In this context we always have the following implications:

$$P \text{ locally closed} \implies P \text{ primitive} \implies P \text{ rational.}$$

So the interesting direction is whether rational prime ideals are locally closed.

When this final implication holds, we say that the ring R satisfies the *Dixmier-Moeglin equivalence*, DME for short.

So what happened after the work of Dixmier and Moeglin?

People started to notice that the equivalence of Dixmier and Moeglin holds more generally. It was shown that the DME holds for:

- finitely generated algebras satisfying a polynomial identity;
- (Zalesskii) group algebras of finitely generated nilpotent-by-finite groups;
- (Ken Goodearl and Ed Letzter) many quantum algebras.

We should point out that many of these examples are examples of Hopf algebras. Since Hopf algebras have additional structure, which often makes them better behaved, it is natural to ask whether the Dixmier-Moeglin equivalence holds for finitely generated noetherian Hopf algebras.

Lorenz's example

Martin Lorenz found an example of a noetherian Hopf algebra for which the DME does not hold. It's not hard to explain either. We start with $H = \mathbb{Z}^2$. Now let $A \in \mathrm{SL}_2(\mathbb{Z})$ be a matrix that has an eigenvalue > 1 in modulus. Then A gives us an automorphism σ of H. Then we take a semidirect product $G := H \rtimes_\sigma \mathbb{Z}$.

Then $\mathbb{C}[G]$ does not satisfy the Dixmier-Mogelin equivalence. In fact, (0) is a rational ideal (and primitive) and it is not locally closed!

What's going on with Lorenz's example?

We have $\mathbb{C}[H] \cong \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$. The automorphism σ corresponds to an automorphism of $(\mathbb{C}^*)^2$. Now if we look at subvarieties that are invariant under σ, we see that because the matrix A has an eigenvalue > 1 in modulus, we get periodic points of arbitrarily large order and these points are Zariski dense. These periodic points give rise to an infinite set of prime ideals above (0) whose intersection is (0).

Lorenz' example looks like a Laurent polynomial ring $\mathbb{C}[x^{\pm 1}, y^{\pm 1}, z^{\pm 1}]$, but where we alter the multiplication slightly to make z not commute with the other variables.

What Lorenz's counterexample shows is that even just for commutative polynomial rings (or, more accurately, Laurent polynomial rings) when one changes the multiplication rule slightly, it is very difficult to know whether the Dixmier-Moeglin equivalence holds.

But this leads to a different question: how does one deform the multiplication of a polynomial ring $R[t]$?

This is where one gets into so-called skew polynomial rings.

The rings $R[t;\sigma,\delta]$

If R is a commutative noetherian ring and t is an indeterminate, then one can produce a noncommutative (skew) polynomial ring $R[t;\sigma,\delta]$ by giving:

- a ring automorphism $\sigma : R \to R$;
- a σ-derivation $\delta : R \to R$ (i.e., δ now satisfies $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$).

One can then deform the multiplication by keeping the same multiplication as before on R and declaring that

$$t \cdot r = \sigma(r)t + \delta(r).$$

One can check this does indeed give us a ring! In the case that $\delta = 0$ we just write $R[t;\sigma]$ and when σ is the identity, δ becomes an ordinary derivation and we write $R[t;\delta]$.

Even in this very special situation, many interesting geometric problems arise when looking at the Dixmier-Moeglin equivalence.

To give an idea, I'll look at what happens in the case $R[t;\sigma]$.

If one looks at $R[t;\sigma]$ with R a finitely generated commutative $\mathbb{C}$-algebra, one can look at this geometrically by looking at the scheme $X = \mathrm{Spec}(R)$ and the induced automorphism $\phi := \sigma^*$ given by $\sigma^*(P) = \sigma^{-1}(P)$. The Dixmier-Moeglin equivalence can be reformulated purely geometrically as follows.

GEOMETRIC DME: automorphism case

The Dixmier-Moeglin equivalence holds for $R[t;\sigma]$ if and only if the following equivalences hold for ϕ-invariant subvarieties of Y of X:

- (primitivity) there is a hypersurface H of Y such that $Z \subseteq \bigcup_{n\in\mathbb{Z}} \phi^n(H)$ for every proper ϕ-invariant subvariety Z of Y;
- (locally closed) the union of proper ϕ-invariant subvarieties of Y is a proper Zariski closed subset of Y;
- (rationality) there does not exist a dominant rational map $f : Y \to \mathbb{A}^1$ such that $f \circ \phi = f$.

That last condition is saying we can't have a commuting diagram

$$\begin{array}{ccc} X & \stackrel{\phi}{\to} & X \\ \downarrow & & \downarrow \\ \mathbb{A}^1 & \stackrel{\mathrm{id}}{\to} & \mathbb{A}^1, \end{array}$$

where the map from X to $\mathbb{A}^1$ has infinite image.

This is a bit hard to wrap one's head around when seeing it for the first time. Let's just focus on $Y = X$ (as it turns out you can always reduce to this case).

Then primitivity in this setting is saying that there is a hypersurface H of X such that the ϕ-orbit of H contains all proper ϕ-invariant subvarieties on X.

Locally closed is saying that the union of the proper ϕ-invariant subvarieties is itself a proper and ϕ-invariant subvariety; i.e., there is a maximal proper ϕ-invariant subvariety of X.

Rational is just saying that we shouldn't be able to partition X into an uncountable set of ϕ-invariant hypersurfaces (the fibres of a map $f : X \to \mathbb{A}^1$).

So we go back to a question of Jordan, which we'll state in geometric language. Let $X = (\mathbb{C}^*)^m$ and let $\phi : X \to X$ be an automorphism. Does one have that primitivity and locally closed are equivalent in this setting?

Ring theoretically, he was asking whether primitive ideals in $R = \mathbb{C}[t_1^{\pm 1}, \ldots, t_m^{\pm 1}][x; \sigma]$ are precisely those prime ideals in $\mathrm{Spec}(R)$ that are locally closed in the Zariski topology.

Technically, he only asked the question for the case $R = \mathbb{C}[t_1^{\pm 1}, t_2^{\pm 1}][x; \sigma]$, and σ was a specific automorphism. This question was answered by Ken Goodearl in 2018 using work of Bombieri, Masser, and Zannier. It was also answered more generally by Dragos Ghioca and me in the same year.

Jordan's original motivation was to produce a counter-example to the Dixmier-Moeglin equivalence. He realized that if he could prove this conjecture then he could produce a counterexample of the form $R = \mathbb{C}[t_1^{\pm 1}, t_2^{\pm 1}][x; \sigma]$. (Historically, this was probably around the same time as Lorenz found his counterexample)

Geometrically, Jordan's question asks whether one of the following statements must necessarily hold:

(A) there is a proper subvariety $Z \subset X$, which contains all the proper, irreducible, ϕ-invariant subvarieties of X.

(B) there is no proper subvariety $Z \subset X$, which contains some iterate of each proper, irreducible, periodic subvariety of X.

Here Y being periodic just means that $\phi^m(Y) = Y$ for some $m \geq 1$.

With Dragos Ghioca, we answered a more general version of the following question:

Theorem (B-Ghioca) Let G be a semiabelian variety defined over an algebraically closed field K of characteristic 0 and let $\Phi : G \to G$ be a dominant, regular self-map. Then one of the following two statements must hold:

(A) there is a proper subvariety $X \subset G$, which contains all the proper, irreducible, periodic subvarieties of G (under the action of Φ).

(B) there is no proper subvariety $Y \subset G$, which contains some iterate of each proper, irreducible, periodic subvariety of G.

As a consequence, we get the following result.

Corollary: (B-Ghioca 2019) Let G be a semiabelian variety defined over an algebraically closed field K of characteristic 0 and let Φ be a dominant group endomorphism of G. Then there is no proper subvariety of G which intersects the orbit of each periodic point of Φ.

Why?

Let's look at the special case when Φ is an automorphism. Look at torsion points.

What is a semiabelian variety?

I should probably explain why this answers the question of Jordan.

You probably know what an abelian variety is (or at least what an elliptic curve is). A semiabelian variety is a bit more general. But let's do a crash course on algebraic groups to say what this is.

An algebraic group is just a group object in the category of algebraic varieties. So let X be a complex quasi-projective variety. We say that X is an algebraic group if there is are morphisms $\mu : X \times X \to X$ (multiplication) and $i : X \to X$ (inversion) such that the usual group axioms hold.

An example is $X = \mathbb{C}^* \cong V(xy - 1) \subseteq \mathbb{A}^2$. Then $\mu : X \times X \to X$ given by $(a, b) \mapsto ab$ and $i : X \to X$ given by $a \mapsto a^{-1}$ give this variety a group structure. We can also do examples like $(\mathbb{C}^*)^m$ with $m \geq 1$. We'll call such a group a torus.

An important result of Chevalley says that if G is an algebraic group then we have a short-exact sequence

$$1 \to N \to G \to A \to 1,$$

where A is an abelian variety (projective) and N is a characteristic connected linear group.

A semiabelian variety is just an algebraic group where N is a torus. Semiabelian varieties are always abelian but they're not necessarily *abelian*. Does that make sense?

In the case that A is just a point, we get tori as a special subclass of semiabelian varieties, so restricting to this case and when the endomorphism is an automorphism answers Jordan's question.

Connection to algebraic dynamics

Even though the original motivation for our question was ring theoretic, there are strong connections to arithmetic dynamics, which we now explain.

Let X be a complex projective variety and let $\Phi : X \to X$ be a dominant endomorphism. We say that Φ is *polarizable* if there exists an ample line bundle $\mathcal{L}$ on X such that $\Phi^*\mathcal{L}$ is linearly equivalent with $\mathcal{L}^{\otimes d}$ for some $d > 1$. Intuitively, d is a bit like a degree and X is a bit like projective n-space.

In this setting, Fakhruddin proved that the periodic points are dense. Furthermore, a more careful analysis of the proof of Fakhruddin's proof yields the existence of a set S of periodic points of X with the property that choosing a point from the orbit of each point in S would always yield a Zariski dense set in X.

Notice this shows that (B) from above must hold in this setting:

(B) there is no proper subvariety $Y \subset X$, which contains some iterate of each proper, irreducible, periodic subvariety of X.

Dynamical Manin-Mumford

Next we discuss the connections with the Dynamical Manin-Mumford conjecture. The original form of the Dynamical Manin-Mumford conjecture, formulated by Zhang in early 1990s says that for a polarizable dynamical system (X, Φ) defined over the complex numbers, if $V \subset X$ is a subvariety which contains a Zariski dense set of preperiodic points, then V must be preperiodic itself; i.e., $\Phi^n(V) \subseteq \overline{\Phi^m(V)}$ for some $n > m$.

The DMM has since been amended and there is a variant that is expected to hold for more general dynamical systems beyond polarizable ones. As it turns out, DMM implies the equivalence of (A) and (B) from above. Therefore we can make the following conjecture.

Conjecture: Let X be a quasiprojective variety defined over an algebraically closed field K of characteristic 0 and let $\Phi : X \to X$ be a dominant, regular self-map. Then one of the following two statements must hold:

(A) there is a proper subvariety $X \subset G$, which contains all the proper, irreducible, periodic subvarieties of G (under the action of Φ).

(B) there is no proper subvariety $Y \subset G$, which contains some iterate of each proper, irreducible, periodic subvariety of G.

A word about the proofs

Our proofs are related to work on the Medvedev-Scanlon conjecture, which predicts that for a dominant rational self-map Φ of a quasiprojective variety X defined over an algebraically closed field K of characteristic 0, either there exists a point $x \in X(K)$ with a Zariski dense orbit, or there exists a non-constant rational function $f : X \to \mathbb{P}^1$ such that $f \circ \Phi = f$. Notice the later condition is related to the rationality condition from before.

This conjecture is known to hold when K is uncountable, but it is very difficult in the case of countable fields.

The proof goes via reduction to the abelian variety case and the torus case, which are dealt with separately. Endomorphisms can be understood as compositions of translations and group endomorphisms. One can reduce to the case of composition of a translation with a unipotent endomorphism. We then borrow (or steal) an argument from Rogalski, Reichstein, and Zhang on wild automorphisms of abelian varieties to handle this case in the abelian variety case. In the torus case one can reduce to the group endomorphism case. Here one looks at torsion points and uses reduction-mod-p techniques.

Thanks.