PCMI Summer School (not quite) notes

Danny Krashen

draft date: July 24, 2024

Contents

Preface

Every time I commit to doing something like these lectures, in some sense I use it as an opportunity(?) to justify my existence. What are the things which I believe are of interest and why? How do we study these things?

The answers I'll present are a bit indirect. For the first, consider the following story[1]. Once upon a time, a young person in the village decides to find out about the meaning of destiny and fate and becomes a wanderer. They travel far and wide. Eventually they are told that if they really want to understand the meaning of life, they should seek out a certain hermit, living in a cave on the side of a mountain. Apparently for many years, the hermit secluded themselves in the search for the meaning of life.

So the wanderer eventually tracks down the hermit, after long toil, and then asks "Master, what is fate?" The master replies "It is that which we carry with us, what we bring from place to place our lives. It is that which causes the toil of beasts of burden. It is that which men in former times had to bear upon their backs. It is that which has caused nations to build byways from City to City upon which carts and coaches pass, and alongside which inns have come to be built to stave off Hunger, Thirst and Weariness." "And that is Fate?" said the wanderer. "Fate? I thought you said freight," responded the hermit. "That's all right," said the wanderer. "I wanted to know what freight was too."

I have found on the search for deep meaning in mathematics, one generally has to carry a lot of freight along the way. And I therefore ask your patience in the beginning of the lectures.

For the how, as to what methods I have found useful, I would say that my main tool has been pure desperation. To me it feels like there has been no method, but rather a frantic stringing together of tools.

Nonetheless, I will try to present things with a polite fiction of coherence, as best I can.

[1] this story, which I attribute to my father, is actually shamelessly modified from "The Profit," by Kehlog Albran (actually written by Martin A. Cohen and Sheldon Shacket).

Chapter 1

Philosophical meanderings around field arithmetic

Let's start with the basic question: for a field F, which systems of polynomial equations have solutions?

As we learn from algebraic geometry, thinking of a variety as a specific collection of equations can be somewhat problematic. Instead, we often learn more from other descriptions and interpretations of such systems. Nonetheless, let us start from this perspective.

As linear equations are not particularly interesting from our perspective – we can very easily answer questions of which linear systems of equations have nontrivial solutions by computing their dimension, we find that the first case of interest is quadratic equations (in possibly many variables).

1.1 Quadratic forms

As many of us know, quadratic forms have an unreasonably rich structure arithmetically, while geometrically, they don't vary in moduli. That is, over an algebraically closed field, any two nonsingular quadratic forms are equivalent after a change of variables, and singular ones are classified entirely by their "amount of singularity" as is encoded in their "radical." On the other hand, over a non-algebraically closed field, there is very rich classification of quadratic forms with incredibly subtle information encoded within them.

We say that forms q, q' are isometric if they differ by an invertible linear change of variables.

We say that a quadratic form q over a field F is isotropic if there is a (projective) solution to the equation $q = 0$, and we say it is anisotropic otherwise.

1.1.1 Overview of some classical results to frame study

1. Hasse-Minkowski, Lagrange

2. u-invariants, finite fields, function fields
3. Kaplansky's conjecture about u-invariants, results of Merkurjev, Vishik, Izbholdin
4. expected behavior of u-invariants over "reasonable" fields
5. Results of Parimala/Suresh, HHK, Leep for p-adics
6. Conjectures for function fields over number fields

1.1.2 The Witt ring of anisotropic forms, fundamental ideal and the Milnor conjectures

1. Grothendieck-Witt ring, Witt decomposition/equivalence, Witt ring, fundamental ideals
2. Ring structure for bilinear forms
3. embedding of $\mathbb{Z}$ into $W(F)$, torsion and nonreality
4. Pfister forms and the powers of the fundamental ideals
5. Galois cohomology – derived functor of Galois fixed points of groups with continuous Galois actions
6. H^0 and H^1 (via crossed homomorphisms), classical invariants of quadratic forms

Pfister number problem (with and without fixed dimension of form) due to Brosnan, Reichstein and Vistoli, 2010.

1.2 Cubic forms

1.2.1 Homogenous 2-variable forms

One variable cubic forms / homogeneous two-variable cubic forms are cubic field extensions. The study of these breaks up into two pieces: their discriminant, which are quadratic extensions, and cubic extensions with fixed discriminant, which are governed by (twisted) Kummer theory.

We see that, in particular, cubic extensions are not all "the same kinds of things," but rather there are certain special ones – cyclic extensions and Kummer extensions – which exhibit special extra structure. We can interpret these via Galois cohomology.

- Kummer sequence, Kummer extensions
- Cyclic extensions

Here we find a common theme: for a certain class of variety – here actually a finite scheme – we have a close relationship with a class of algebraic objects, by which we mean a "linear algebraic object." It is then natural to ask the extent to which we can classify such varieties via those same algebraic structures. Parametrizing Kummer extensions is straightforward, but there is already some subtlety here already in describing cyclic extensions.

In our case, we can indeed write them down and there are various formulations, but they aren't "obvious." For example:

$$f(X) = X^3 - tX^2 + (t-3)X + 1$$

for any value of $t \in F$ has splitting field which is a cyclic degree 3 extensions and conversely, every degree 3 cyclic extension has an element with a minimal polynomial of this form.

Finding such expressions for cyclic extensions of higher degree is not so simple. Indeed, one can show that no such straightforward parametrization can work for the group C_8.

But all this concerns homogeneous polynomials in 2 variables. What about 3 or more variables?

1.2.2 Homogeneous cubic forms in more variables

We can clearly see that the case of 3 variables in degree 3 is particularly special. These are genus 1 plane curves which includes the case of elliptic curves. In particular, there are both geometric as well as arithmetic aspects of these curves – even over an algebraically closed field, these are not all isomorphic but are classified by a 1-dimensional moduli (the j-line). Singular ones have highly constrained behavior (cusp or node) the normalizations of which are rational curves with a single singularity (node or cusp) and with the complement rationally parametrized. Consequently thier normalizations are just the projective line, and these don't vary in moduli.

There are also further famous advantages to studying these from an arithmetic perspective, but we will mostly not consider such things.

For now, we will put these aside as a different kind of "nonlinear phenomena."

How about the case of 4 variables? Here we find a new kinds of phenomena.

Generically a cubic form in 4 variables determines a cubic surface, which have rich arithmetic. Unlike the case of quadratic forms, cubic forms have moduli – this is to say, even over an algebraically closed field

Given a cubic field extension E/F, we can consider the equation $N_{E/F}(x) = b$ for some $b \in F^*$. The vector space E is 3 dimensional and this gives, after homogenization, a degree 3 form in 4 variables. At the algebraic closure, this looks like $xyz = w^3$, a form which is singular when w and any other variable equals 0. Such an equation has some very interesting behavior.

1. examination of the degree 2 case of this and quaternion algebras

2. examination of the degree 3 case of this for cyclic extensions and cyclic/symbol algebras

what is the "natural algebraic structure" if we don't have a cyclic extension??? Not clear.

1.3 Generalizations via algebraic structures

1. Cyclic algebras, norms
2. Central simple algebras, Crossed products, Galois cohomology
3. Brauer group, division algebras

Analog of the u-invariant – period-index problem. How large can an "anisotropic" central simple algebra be with a given period?

relationship with u-invariant via clifford invariant: via Merkurjev's theorem, u-invariant bound gives period-index bound for period 2 classes.

Period-index conjectures of Colliot-Thelene.

Chapter 2

Measurements of field arithmetic

2.1 Galois cohomology and field arithmetic

2.1.1 The many faces of Galois cohomology

We'll give a quick summary of group cohomology, Milnor K-theory and motivic cohomology and describe thier interrelationships. In some sense, this is pedagogically backwards – these are, in some sense, the tools we will use to study fields and algebraic structures over them, and it would therefore be more natural to start with these algebraic structures. Instead, we'll discuss these in Section 2.2.

2.1.1.1 Galois cohomology

The definition of Galois cohomology is straightforward. Let k be a field, G_k its absolute (profinite) Galois group, and Ab_{G_k} the category of Abelian groups endowed with a (usually discrete) topology and a continuous action by G_k. For $M \in Ab_{G_k}$, the invariants M^{G_k} gives a left exact functor to Abelian groups, and we define the Galois cohomology group $H^n(G_k, M)$ to be the nth right derived functor of this functor. The category Ab_{G_k} has a natural monoidal structure extending $\otimes_{\mathbb{Z}}$ on Abelian groups, and the Galois cohomology groups are endowed with a cup product $H^n(G_k, M) \otimes_{\mathbb{Z}} H^m(G_k, N) \to H^{n+m}(G_k, M \otimes_{\mathbb{Z}} N)$. These groups have remarkable connections to various algebraic structures.

A particularly important role is played by the groups $H^n(k, \mu_\ell^{\otimes n})$, which, as n varies, form a ring. By convention, we set $\mu_\ell^{\otimes 0} = \mathbb{Z}/n$ so that $H^0(k, \mu_\ell^{\otimes 0}) = \mathbb{Z}/n$. Hilbert 90 tells us that $H^1(k, \mathbb{G}_m) = H^1(k, (k^{\text{sep}})^*) = 0$, which tells us $H^1(k, \mu_\ell) \cong k^*/(k^*)^\ell$. We conventionally write (a) of $(a)_\ell$ to denote the element of $H^1(k, \mu_\ell)$ corresponding to the class of a in $k^*/(k^*)^\ell$. Cup products of these elements are

written by concatenation, so that $(a) \cup (b) = (a, b)$ and $(a_1, \ldots, a_m) \cup (a_{m+1}, \ldots, a_n) = (a_1, \ldots, a_n)$. These elements are caled symbols.

As a wider context, the Galois cohomology groups coincide with étale cohomology: if X is a scheme and $\mathscr{F}$ is a sheaf in the étale topology, we can define $H^n_{\text{ét}}(X, \mathscr{F})$. In the case that $X = \operatorname{Spec} k$, we have $H^n_{\text{ét}}(k, \mathscr{F}) = H^n_{\text{ét}}(\operatorname{Spec} k, \mathscr{F}) = H^n(G_k, \mathscr{F}(k^{\text{sep}}))$.

2.1.1.2 Milnor K-theory

The the definition of Galois cohomology was straightfowards, the definition of Milnor K-theory is surprisingly more so. For a field k, we define the Milnor K-theory ring $K^M_\bullet(k) = \oplus_n K^M_n(k)$ by:

1. $K^M_0(k) = \mathbb{Z}$,
2. $K^M_1(k) \cong k^*$ written additively. That is, the elements of $K^M_1(k)$ are written as $\{a\}$ for $a \in k^*$ with the additive structure $\{a\} + \{b\} = \{ab\}$,
3. products are written by concatenation. That is: $\{a\}\{b\} = \{a, b\}$ and

   $$\{a_1, \ldots, a_m\}\{a_{m+1}, \ldots, a_n\} = \{a_1, \ldots, a_n\}$$

   (these elements are called symbols),
4. the ring structure is the free associative one described above, but modulo the relations $\{a, b\} = 0$ whenever $a + b = 1$.

The relationship with Galois cohomology can be seen from the fact that $(a, b)_\ell = 0$ in $H^2(k, \mu_\ell^{\otimes 2})$ whenever $a + b = 1$, which provides a natural map

$$K^M_\bullet(k) \to K^M_\bullet(k)/\ell \xrightarrow{\mathscr{N}} H^\bullet(k, \mu_\ell^{\otimes \bullet})$$

where $\mathscr{N}$ is refered to as the norm residue map (due to Tate?). The key result of Voevodsky and others (Weibel, Suslin, Rost, ...) is that this is an isomorphism. This was known as the Bloch-Kato conjecture.

While these have an astonishingly elementary presentation, and have a number of natrual maps and properties (restriction, corestriction, residues, specializations, reciprocity, etc), they don't obviously generalize beyond fields to schemes.

2.1.1.3 The Witt ring

The Witt ring encodes information about quadratic forms over a field. Recall that for a vector space V over a field k of characteristic not 2, the polarization identities let us pass between quadratic forms and symmetric bilinear forms, which give rise to homomorphisms $V \to V^*$. We say that a form is nonsingular if this is an isomorphism. The Witt ring $W(k)$ is defined as

- generated as an Abelian group by $q = (V, q) = (V, b)$ consisting of a vector space with a bilinear form,
- modulo the ideal generated by $(V \perp W) - V - W$ and by the form xy (the hyperbolic plane),
- with ring structure given by the tensor product (and corresponding bilinear form).

This group contains and enriched version of the Galois cohomology ring with $\mathbb{Z}/2$ coefficients, thanks to the Milnor conjecture, proved by Voevodsky. The connection works like this. By Gram-Schmidt, we may, after change of basis, write a nonsingular quadratic form in the form $q(x_1, \ldots, x_n) = a_1x_1^2 + \cdots, +a_nx_n^2$, and we write this form as $\langle a_1, \ldots, a_n\rangle$. We write $\langle\langle a\rangle\rangle = \langle 1, -a\rangle$ and $\langle\langle a_1, \ldots, a_n\rangle\rangle = \langle\langle a_1\rangle\rangle \otimes \cdots \otimes \langle\langle a_n\rangle\rangle$. These are called n-fold Pfister forms.

We define $I(k)$ to be the ideal of $W(k)$ consisting of even dimensional forms, and $I^j(k)$ it's jth power. It turns out that I^j is generated by j-fold Pfister forms, and that one may obtain a homomorphism

$$K_j^M(k) \to I^j(k)/I^{j+1}(k)$$

defined by taking the symbol $\{a_1, \ldots, a_j\}$ to the Pfister form $\langle\langle a_1, \ldots, a_n\rangle\rangle$ induces an isomorphism

$$K_j^M(k)/2 \cong I^j(k)/I^{j+1}(k).$$

This was known as the Milnor conjecture and was proved by Voevodsky. This gives rise to a series of (surjective) maps:

$$e_j : I^j(k) \to K_j^M(k)/2 \to H^j(k, \mu_2)$$

These are particularly useful for understanding these cohomology groups, as it says that every mod 2 cohomology class is determined by a quadratic form, giving useful tools to approach them.

2.1.1.4 Motivic cohomology and motivic complexes

A key feature of Milnor K-theory, is that (due to the Bloch-Kato conjecture), is that $K_n^M(k)$ provides an "integral version" of the étale cohomology groups $H^n(k, \mu_\ell^{\otimes n})$. On the other hand, this is specific to the coefficients $\mu_\ell^{\otimes n}$ in degree n cohomology. Among other things, motivic cohomology provides integral versions of various cohomology groups, including powers of roots of unity.

The essential feature here was the construction of the so-called motivic complexes, typically denoted $\mathbb{Z}(m)$. These are particular complexes of presheaves on the category of smooth schemes over a field k, and are usefully considered both with respect to the étale, Zariski (or Nisnevich) topologies. The Zariski hypercohomology groups $\mathbb{H}^n(X, \mathbb{Z}(m)) = H^n(X, \mathbb{Z}(m)) = H^{n,m}(X, \mathbb{Z})$ and is the (n, m)th motivic cohomology group of X. The étale hypercohomology groups, denoted $H^n_{\text{ét}}(X, \mathbb{Z}(m))$ are called the étale motivic cohomology groups. These relate to the other groups in the following ways:

1. there is a quasi-isomorphism $\mu_\ell^{\otimes n} \to \mathbb{Z}/\ell(n)$ in the **étale** topology (for example, Theorem 10.3 in Mazza-Voevodsky-Weibel),

2. there is an isomorphism $H^n_{\text{Zar}}(k, \mathbb{Z}(n)) = K^M_n(k)$ (Nestrenko-Suslin in 1990 / Totaro in 1992 in the context of Bloch's higher Chow groups, for example).

3. the Bloch-Kato conjecture can be seen as an identification of $H^n_{\text{Zar}}(k, \mathbb{Z}/\ell(n))$ and $H^n_{\text{ét}}(k, \mathbb{Z}/\ell(n))$, which follows from the Beilinson-Lichtenbaum conjecture, saying that the pushforward from étale to Zariski (or Nisnevich) is acyclic for $\mathbb{Z}/\ell(n)$ up to degree n (for any smooth variety over k) this is, roughly, $H^m_{\text{Zar}}(k, \mathbb{Z}/\ell(n)) \cong H^m_{\text{ét}}(k, \mathbb{Z}/\ell(n))$ for $m \leq n$.

2.1.1.5 Overview/Summary

1. Galois cohomology naturally arises in looking for invariants of algebraic objects and varieties (cohomological invariants, birational invariants of varieties, etc). Generalizes to étale cohomology of schemes.

2. Milnor K-theory has a remarkably simple presentation in terms of generators and relations. Also has various useful properties/ natural operations (residues, restriction, corestriction, specialization, reciprocity). Doesn't generalize easily beyond fields (some results for certain rings, though).

3. Motivic cohomology glues together the two things above, and relates to a number of other geometric theories/constructions (for example Chow groups), and have cohomological operations, providing tools for relating invariants in new ways.

2.1.2 Interactions with field arithmetic

If these various groups (motivic cohomology groups, étale cohomology groups, etc) play a role similar to cohomology groups of a topological space, for example, we should be able to use them to study arithmetic properties of fields. In addition, as we will see in the next section, they can be used to measure invariants of algebraic structures.

2.1.2.1 The dimensions of a field and splitting forms

There is no single notion of the "dimension" of a field. Instead, we have a series of competing notions, which do not always agree with each other.

2.1.2.1.1 Naive/heuristic dimension

Definition 2.1.2.1. *For k a finitely generated over a prime field or an algebraically closed field k_0, we say the (naive) dimension* $\dim(k)$ *is:*

- $\text{trdeg}_{k_0}(k)$ *if k_0 is algebraically closed,*

- $\mathrm{trdeg}_{k_0}(k) + 1$ *if* k_0 *is finite,*
- $\mathrm{trdeg}_{k_0}(k) + 2$ *if* $k_0 = \mathbb{Q}$.

A very rough rationalle for this (really quite ad hoc) is that we are trying to model fields which have properties analogous to function fields of varieties over algebraically closed fields, as in the first part of the definition. A finite field, in terms of its Galois theory, is quite similar to $\mathbb{C}((x))$, which both have unique cyclic extensions of any given degree, with an absolute Galois group of $\widehat{\mathbb{Z}}$. In this sense, it behaves like something which would be "geometrically dimension 1." Global fields (function fields of curves over finite fields) should then have dimension two, and number fields, as they are analogous to global fields, should also have dimension 2.

2.1.2.1.2 Cohomological dimension

Definition 2.1.2.2. *We say that the cohomological dimension of a field k is at most n if for every discrete, torsion G_k module M, we have $H^m(G_k, M) = 0$ whenever $m > n$. We say* $\mathrm{cdim}(k) = n$ *if n is the infemum of the set of integers such that k has cohomological dimension at most n.*

Examples: finite fields have $\mathrm{cdim}(k) = 1$. Global fields and imaginary number fields have $\mathrm{cdim}(k) = 2$. More generally, for finitely generated fields which are not formally real (-1 is a sum of squares), we have $\mathrm{cdim}(k) = \dim(k)$. The presence of real orderings makes the cohomological dimension act quite differently than the naive dimension. In fact, if a field has real orderings, the cohomological dimension is always infinite! To take this into account, one can alternatively consider the virtual cohomological dimension: this is defined to be the cohomological dimension of $k(\sqrt{-1})$.

2.1.2.1.3 Diophantine dimension and Tsen rank

Definition 2.1.2.3. *We say that a field k is C_n if for every $d > 0$ and $m > d^n$, every homogeneous polynomial f of degree d in m variables has a nontrivial zero. We say the Diophantine dimension of k is n and write* $\mathrm{ddim}(k) = n$ *if n is the smallest integer such that k is C_n.*

Definition 2.1.2.4. *We say that a field k is T_n if for every $d_1, \ldots, d_r > 0$ and $m > \sum d_i^n$, every system of homogeneous polynomials f_i with* $\deg f_i = d_i$ *in m variables has a nontrivial zero. We say the Tsen rank of k is n, and write* $\mathrm{trk}(k) = n$ *if n is the smallest integer such that k is T_n.*

Clearly $T_n \implies C_n$ and so $\mathrm{trk}(k) \geq \mathrm{ddim}(k)$. The converse is open. For finitely generated fields over $\mathbb{Q}$, $\mathrm{ddim}(k)$ is not finite, but for finitely generated fields over finite fields or algebraically closed fields, one has $\dim(k) = \mathrm{cdim}(k) = \mathrm{ddim}(k)$.

Examples of Ax show that it is possible to have fields of cohomological dimension 1, but infinite Diophantine dimension (and hence Tsen rank). The converse is much less clear:

Question 2.1.2.5 (Serre, Galois cohomology)**.** *Is* $\mathrm{ddim}(k) \geq \mathrm{cdim}(k)$*?*

This is perhaps motivated by the following idea:

Definition 2.1.2.6. *Let* $\alpha \in H^n(k, A)$*. We say that a homogeneous polynomial* f *is a splitting form for* α *if for every field extension* L/k*,* $\alpha_L = 0$ *whenever* f_L *is isotropic.*

One can show, for example, that a positive answer to Serre's question would follow from the existence of splitting forms of degree ℓ and in $\ell^n + 1$ variables for symbols $\alpha \in H^n(k, \mu_\ell^{\otimes n})$ (in fact, it suffices to consider the case that ℓ is a prime, and that k is prime-to-ℓ closed). This holds for $n = 2$ (the Severi-Brauer varieties), $n = 3$ (Merkurjev-Suslin varieties), n general and $\ell = 2$ (Pfister quadrics, thanks to the positive solution to the Milnor conjecture), $n = 4, \ell = 3$ (Norm equations for Albert algebras), but these are not known to exist in general.

In fact, for a given value of $\mathrm{ddim}(k)$, $\mathrm{cdim}(k)$ is not known to be bounded in general. In work with Matzri, we have shown that if $\mathrm{ddim}(k)$ is finite, then for every p, the p-torsion in $H^i(k, M)$ only occurs for i roughly up to $\log_2(p)\,\mathrm{ddim}(k)$. In the case $p = 2$, this gives the conjectural description, but we don't get any uniform result for different p...

There are a number of related properties and variations of the above. These include the $\mathscr{A}_i$ properties of Leep, and the $C_{i,j}$ property of Kato / Kato-Kazumaki.

2.1.3 Structural problems in Galois cohomology

In this section we will be considering different notions of complexity of algebraic objects.

2.1.3.1 The period-index problem

Given a field k and a cohomology class $\alpha \in H^i(k, \mu_\ell^{\otimes j})$, we say that a field extension L/k splits α if $\alpha_L = 0$ in $H^i(L, \mu_\ell^{\otimes j})$.

Definition 2.1.3.1. *For* α *as above, we set*

$$\mathrm{ind}(\alpha) = \gcd\{[L : k] \mid L/k \text{ is a finite field extension splitting } \alpha\}$$

$$\mathrm{per}(\alpha) = \text{ the order of } \alpha \text{ in } H^i(k, \mu_\ell^{\otimes j})$$

Of course $\mathrm{per}(\alpha)$ is bounded by ℓ. A restriction-corestriction argument shows that $\mathrm{per}(\alpha) | \mathrm{ind}(\alpha)$, and one may also show $\mathrm{ind}(\alpha) | \mathrm{per}(\alpha)^N$ for some integer N (depending possibly on α).

Problem 2.1.3.2 (The period-index problem)**.** *For a given field* k*, and integers* i, j, ℓ*, find an integer* n *(for example, in terms of* $\mathrm{ddim}(k)$ *or* $\dim(k)$ *in the finitely generated case) such that* $\mathrm{ind}(\alpha) | \mathrm{per}(\alpha)^n$ *for all* $\alpha \in H^i(k, \mu_\ell^{\otimes j})$*.*

Conjecture 2.1.3.3 (The period-index conjecture for degree 2, often attributed to Colliot-Thélène)**.** *For a field k with* $\mathrm{ddim}(k) = n$ *or* $\dim(k) = n$ *and* $\alpha \in H^2(k, \mu_\ell)$*, we have* $\mathrm{ind}(\alpha) | \mathrm{per}(\alpha)^{n-1}$*.*

In many cases of interest, no such bound is known to exist, for example for finitely generated fields over $\mathbb{Q}$ of transcendence degree at least 1. On the other hand, the well known result of Albert-Brauer-Hasse-Noether for the Brauer group shows that $\mathrm{per}(\alpha) = \mathrm{ind}(\alpha)$ for $\alpha \in H^2(k, \mu_\ell)$ for k a global field.

2.1.3.2 Essential and canonical dimensions

Having decided on a class of algebraic objects – be it central simple algebras, quadratic forms, etc, it is natural to think of these as giving a functor which associates to a field (or ring), the isomorphism classes of algebraic objects over this field (or ring). We therefore recall some measures of complexity for functors.

2.1.3.2.1 Essential dimension

Definition 2.1.3.4. *For a functor $\mathscr{F}$ from field extensions of k to sets, we define the essential dimension of an element $\alpha \in \mathscr{F}(L)$ to be the minimal transcendence degree of a field extension L_0/k with $L_0 \subset L$ such that α is the image of some $\alpha_0 \in \mathscr{F}(L_0)$. We define $ed(\mathscr{F})$, the essential dimension of $\mathscr{F}$ to be the supremum of essential dimensions of $\alpha \in \mathscr{F}(L)$, taken over all field extensions L/k.*

For example, if $\mathscr{F}(L)$ is the isomorphism classes of quadratic forms of a fixed dimension n over L, then any such form, having a diagonal representation $\langle a_1, \ldots, a_n \rangle$ is defined over the field $k(a_1, \ldots, a_n)$ and hence the essential dimension of $\mathscr{F}$ is at most n (and in fact is equal to n). This captures, in a sense, a notion of complexity of such structures, by giving a "minimal number of parameters" needed to describe these objects.

Definition 2.1.3.5. *For a functor $\mathscr{F}$ from k-algebras to sets, we say that an element $\alpha_0 \in \mathscr{F}(R)$ is versal if for every field extension L/k and $\alpha \in \mathscr{F}(L)$, there exists a k-algebra homomorphism $R \to L$ taking α_0 to α.*

For example, the form $\langle x_1, \ldots, x_n \rangle$ defined over the ring $k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is versal for quadratic forms of dimension n.

Exercise 2.1.3.6. *If there exists $\alpha_0 \in \mathscr{F}(R)$ with R a finitely generated k-algebra which is a domain, then $ed(\mathscr{F})$ is at most the Krull dimension of R.*

Problem 2.1.3.7 (A fundamental (ideal) problem)**.** *Let $\mathscr{I}_n^m(L)$ be isomorphism classes of quadratic forms of a fixed dimension n which lie in $I^m(L)$. Is $ed(\mathscr{I}_n^m)$ finite?*

Note that we may extend this functor to k-algebras by defining it to be those forms which, for every homomorphism to a field (i.e. for each prime) specialize to forms in the fundamental ideal. That is $q \in \mathscr{I}_n^m(R)$ if for every prime $\mathfrak{p}$ with residue field $\kappa(\mathfrak{p})$, we have $q \otimes_R \kappa(\mathfrak{p}) \in I^n(\kappa(\mathfrak{p}))$.

That is, is there a way to present the basic form of a quadratic form in n variables in I^m? The answer is yes if $m = 0, 1, 2, 3$, but this is open for $m > 4$ and $n \geq 2^m + 2^{m-1}$ (it follows from the work of Hoffmann/Vishik that we may obtain a bound if $n < 2^m + 2^{m-1}$)).

2.1.3.3 Canonical dimension

A natural way to approach Problem 2.1.3.7, in light of the Milnor conjecture, is as follows. There is a natural transformation of functors $\mathscr{I}_n^m \to \mathscr{H}^n$ which associates to a quadratic form q over a k-algebra R (let's say regular, or even smooth, to not add too many potential issues), a cohmology class in $H^n_{\text{ét}}(R, \mu_2)$ – it is actually convenient to let $\mathscr{H}^n$ be the Zariski sheafification of this presheaf for this to make sense (we don't need this for $n \leq 2$, but see the work of Esnault, Kahn, Levine, Veihweg for the issues which arise in the case $n = 3$, and in principle, things continue to get more complicated thereafter). We may then obtain an exact sequence of functors

$$0 \to \mathscr{I}_n^{m+1} \to \mathscr{I}_n^m \to \mathscr{H}_n$$

and we can hope to obtain a bound on the essential dimension inductively on powers of the fundamental ideal, if we can bound the ways in which we can split elements of H_n. This leads us to...

Definition 2.1.3.8 (Canonical dimension)**.** *Suppose $\mathscr{F}$ is a functor from field extensions of k to pointed sets. For $\alpha \in \mathscr{F}(L)$, we can associate to this a new functor $\check{\mathscr{F}}_\alpha$ from field extensions of L to sets, defined by $\check{\mathscr{F}}_\alpha(E) = *$ if α maps to the point in $\mathscr{F}(E)$, and $\check{\mathscr{F}}_\alpha = \emptyset$ otherwise. We define $cd(\alpha)$, the canonical dimension of α to be the essential dimension of $\check{\mathscr{F}}_\alpha$.*

Definition 2.1.3.9 (Generic splitting schemes)**.** *For a functor $\mathscr{F}$ from field extensions of k to pointed sets, and $\alpha \in \mathscr{F}(L)$, we say that an L-scheme X is a generic splitting scheme for α if for a field extension E/L, we have $\alpha_E = *$ if and only if $X(E) \neq \emptyset$.*

Exercise 2.1.3.10 (?)**.** *If X is a generic splitting scheme for α of finite type over L, then the canonical dimension of α is at most the Krull dimension of X.*

Problem 2.1.3.11 (Generic splitting schemes)**.** *Do (finite type) generic splitting schemes exist for classes in cohomology groups $H^i(k, \mu_\ell^{\otimes j})$?*

For $\ell = 2$ and α a symbol, the Pfister quadrics are generic splitting schemes, but in general for non symbols, we have no such generic splitting schemes of finite type (except for forms of small Pfister length...). These also exist for symbols in H^3 and H^4 for $\ell = 3$ and $j = i - 1$ (using Albert algebras). In [**?**], these are shown to exist for $i \leq 2$, but this is open in general for $i \geq 3$.

For α a symbol (in the case $i = j$), these exist up to issues of prime to ℓ extensions for ℓ a prime. These are the norm varieties.

For non-symbols in general, things are pretty wide open.

2.1.3.3.1 Representation and Effective indices It is not clear that this notion of index is always the correct one for higher cohomology classes. We may also define the representation index of $\alpha \in H^i(G_k, \mu_\ell^{\otimes j})$ to be the smallest m such that α is the inflation of a class in $H^i(Gal(E/k), \mu_\ell^{\otimes j}(E))$ with $[E : k] = m$. In some ways this may be better behaved.

The effective index is the min over splitting fields.

2.1.3.4 The symbol length problem

Given a cohomology class $\alpha \in H^i(k, \mu_\ell^{\otimes i}) \cong K_i^M(k)/\ell$, due to the explicit presentation of the Milnor K-theory group, we may write $\alpha = \alpha_1 + \cdots + \alpha_m$ for $\alpha_j = (a_{1,j}, \ldots, a_{i,j})$. The minimal such m is called the symbol length of α.

Problem 2.1.3.12 (The symbol length problem)**.** *For a given field k, and integers i, ℓ, find an m (in terms of some kind of dimension of the field, for example) such that the symbol length of every class in $H^i(k, \mu_\ell^{\otimes i})$ is at most m.*

It is not hard to show that a bound on the symbol length gives a bound on the index. More subtle is a partial converse (K): if we have index bounds in degrees up to n, for finite field extensions of k, we obtain symbol length bounds for degree n.

In general though, this problem is pretty wide open. For example, there is no known bound on symbol length for cohomology classes of degree at least 2 over complex function fields in at least 3 variables (with the exception of ℓ a power of 2 from the theory of quadratic forms!!). The problem of function fields over number fields and finite fields is similarly opaque. Some notable results for degree 2 classes on surfaces were obtained by deJong (complex), Lieblich (finite field), p-adic (AAIKL). For degree 3 and higher, very very little is known.

A huge step forward was obtained by Matzri, who showed that the symbol length of a class in $H^2(k, \mu_\ell^{\otimes 2})$ is bounded in terms of $\mathrm{ddim}(k)$, i and ℓ whenever k contains a primitive ℓth root of unity. Conjecturally, however, we expect that there is a bound which doesn't depend on ℓ. In the case that $\mathrm{ddim}\, k = d$, $\ell = p^t$, Matzri gives an upper bound of $t(p^{d-1} - 1)$ for the symbol length.

Problem 2.1.3.13 (The symbol length problem (index version))**.** *For a field k_0, and integers i, ℓ, n, find an m such that the symbol length of every class in $H^i(k, \mu_\ell^{\otimes i})$ which has index dividing n has index at most m, for every field k containing k_0.*

Combined with other results, if $\ell = p^t$, and k_0 has finite characteristic or is algebraically closed, one can use Matzri's results to obtain bounds in the case $i = 2$. Namely, if $\mathrm{ind}(\alpha) = p^s$, we get a symbol length of at most

$$t\left(p^{\left(p^{2s-2}+1+\epsilon\right)} - 1\right)$$

and a lower bound of $\lceil \frac{s}{t} \rceil + 1$.

2.1.3.5 The decomposability problem

In the symbol length problem, it was essential that we were able to write a general cohomology class as a sum of symbols in order for the problem to make sense. For more general cohomology classes $\alpha \in H^i(k, \mu_\ell^{\otimes j})$, it is natural to ask whether or not α may be written as a sum of "simpler" classes. One natural formulation is the following:

Problem 2.1.3.14 (The decomposability problem)**.** *Given a cohomology class $\alpha \in H^i(k, \mu_\ell^{\otimes j})$, can we find classes $\alpha_1, \ldots, \alpha_m$ with $\text{ind}(\alpha_i) = \ell$ and $\sum \alpha_i = \alpha$?*

Again, this is wide open, however in the case ℓ is prime, a result of Merkurjev [**?**] shows that $H^2(k, \mu_\ell)$ is generated by elements of index ℓ. I don't know of any results for other degrees and other twists, though.

I personally expect that classes should decompose in this way, but I have very little evidence to back it up.

On the extreme side of this, one asks if we can write classes in such a way that the index is "accounted for" simply by "independent parts" which compose it:

Problem 2.1.3.15 (The indecomposability existence problem)**.** *Given α of period ℓ and index ℓ^n, can we write $\alpha = \alpha_1 + \alpha_2$ with*

- $\text{ind}(\alpha_1)\,\text{ind}(\alpha_2) = \text{ind}(\alpha)$ *(strong decomposability) or*
- $\text{ind}(\alpha_1), \text{ind}(\alpha_2) < \text{ind}(\alpha)$ *(weak decomposability)*

Once more, very little is known here outside some results in degree 2. The existence of strong indecomposables in degree 2 has a long history, with various classical examples and more recent constructions given by Karpenko as well as by McKinnie. In particular, Karpenko gave methods for detecting decomposability via Chow groups of homogeneous varieties. In work in progress I have some results on weak decomposability, following Karpenko's methods. The higher degree cases are wide open.

The expectation, however, is that decomposable classes should arise as the dimension increases.

2.1.3.6 Index vs effective index

Problem 2.1.3.16. *For $\alpha \in H^i(k, \mu_\ell^j)$ is $\min\{[E : k] | \alpha_E = 0\} = \gcd\{[E : k] | \alpha_E = 0\}$?*

This is answered in the affirmative for $i = 1$ and for $i = 2$, $j = 1$. It is open is essentially all other cases.

2.1.3.7 The cyclicity problem

Problem 2.1.3.17. *Are classes of prime index split by cyclic field extensions of that index?*

This is known in the affirmative for $i = 2, j = 1, \ell \in \{2, 3\}$ and open in essentially all other cases.

2.1.3.8 The admissibility problem

Problem 2.1.3.18. *For a cohomology class $\alpha \in H^i(k, \mu_\ell^j)$, what are the possible groups G which appear as Galois groups of field extensions E/k such that $\alpha_E = 0$?*

This was originallly posed by Schacher in the case $k = \mathbb{Q}, i = 2, j = 1$. Various partial results are known, but it is quite open in general.

2.1.3.9 The genus problem

Problem 2.1.3.19 (one of many variations)**.** *For a cohomology class $\alpha \in H^i(k, \mu_\ell^j)$, determine all classes β such that $\beta_E = 0$ if and only if $\alpha_E = 0$ for E/k finite.*

The collection of such β could be called the genus (or species) of α, and is conjecturally finite for finitely generated fields.

2.2 Complexity of algebraic objects

We have earlier introduced field arithmetic to be the study of solutions to polynomial equations. In practice, these equations often arise from understanding properties of algebraic structures, which we think of as (a collection of) vector space(s) equipped with tensors and maps between them (satisfying some axioms etc).

Often these algebraic objects are described by descent – all twisted forms of some fixed "model" or "split" object, and hence are in bijection with torsors for a linear algebraic group G.

So now, given some type of algebraic structure, we naturally want to ask:

- **Parametrization**: how can we parametrize all such structures, or give some kind of "bounded presentation" for them?
- **Classification**: how can we tell if two of these are the same?

Both of these questions can be interpreted in different ways, and may also interact with each other.

A usual approach to the classification problem is to come up with a collection of invariants, often with values in Galois cohomology. We think of this as like "characteristic classes." Typically these tend to have values in $H^n(k, \mu_\ell^{\otimes(n-1)})$ for various n ("one off" from Milnor K-theory). Given a suitable parameter space, one can consider these invariants as classes on these parameter spaces, as the invariants of a "universal class." A basic example of this would be the following:

- structure: quadratic forms of a fixed dimension d over a field k
- parametrization: as we have seen, we can always diagonalize a quadratic form using the Gram-Schmidt process, and hence a quadratic form is given by parameters $t_1, \ldots, t_d \in k^*$, corresponding to the form $\langle t_1, \ldots, t_d \rangle = \sum t_i x_i^2$.

- classification: one can construct invariants into Galois cohomology, such as the Steifel-Whitney classes, with values in $H^\bullet(k, \mu_2)$. These typically don't characterize the form. We can also interpret these classes as giving cohomology classes in $H^\bullet(k[t_1, \ldots, t_d], \mu_2)$ corresponding to the "generic form" $\langle t_1, \ldots t_d \rangle$ over the ring $k[t_1^{\pm 1}, \ldots, t_d^{\pm 1}]$.

Chapter 3

Some problems

3.1 Quadratic forms

Definition 3.1.0.1. *Let F be a field. We define the fundamental ideal $I(F) \subset W(F)$ to the classes of quadratic forms of even dimension. We let $I^n(F) = (I(F))^n$.*

Definition 3.1.0.2. *For $a \in F^*$, let $\langle\langle a \rangle\rangle$ denote the quadratic form $\langle 1, -a \rangle$. For $a_1, \ldots, a_n \in F^*$, let $\langle\langle a_1, \ldots, p_n \rangle\rangle = \langle\langle a_1 \rangle\rangle \otimes \cdots \otimes \langle\langle a_n \rangle\rangle$. We call such forms n-fold Pfister forms.*

Exercise 3.1.0.3. *Show that $I^n(F)$ is generated by the classes of n-fold Pfister forms.*

Exercise 3.1.0.4. *By Graham-Schmidt, if q is a quadratic form on a vector space V and $v \in V$, we can write $V = Fv \perp W$ for some complementary subspace W. Show that if V is 2 dimensional with $q = \langle a, b \rangle$ and if $v \in V$ with $q(v) = c \in F^*$, then we may write $q = \langle c, abc \rangle$.*

As a hint for the above exercise, consider the determinant of the Graham matrix of the bilinear form associated to q.

Exercise 3.1.0.5. *Show that $\langle\langle a, 1 - a \rangle\rangle$ is hyperbolic.*

Exercise 3.1.0.6. *Show that the map $\widetilde{f} : F^* \times \cdots F^* \to W(F)$ sending $(a_1, \ldots, a_n)$ to $\langle\langle a_1, \ldots, a_n \rangle\rangle$ satisfies $\widetilde{f}(a_1, \ldots, a_n) = 0$ whenever $a_i + a_j = 1$ for some i, j.*

Exercise 3.1.0.7. *Show that $\widetilde{f}$ induces a homomorphism $f : K^M_\bullet(F) \to gr^I_\bullet W(F)$ of graded rings.*

Exercise 3.1.0.8. *Show that $f(2\, K^M_\bullet(F)) = 0$.*

Definition 3.1.0.9. *For a field F, the n'th Pfister number of F, denoted $\mathrm{Pf}_n(F)$, is the minimum number m such that every element of $I^n(F)$ can be written as a sum (or difference/integral linear combination) of at most m n-fold Pfister forms.*

Exercise 3.1.0.10. *Show that the Pfister form $\langle\langle 1, a_2, \ldots, a_n \rangle\rangle$ is always isotropic.*

We will use the following helpful fact: if $\phi = \langle\langle a_1, \ldots, a_n \rangle\rangle$ and if $\phi(x) = b$ has a solution, then we may write $\phi \cong \langle\langle -b, b_2, \ldots, b_n \rangle\rangle$.

Exercise 3.1.0.11. *Show that if ϕ is a Pfister form and $\phi(x) = -1$ has a solution then ϕ is isotropic.*

Exercise 3.1.0.12. *Use the previous exercises to show that if a pfister form is isotropic, then it is hyperbolic.*

Exercise 3.1.0.13. *Show that if ϕ is a Pfister form and ψ is a subform of dimension greater than half the dimension of ϕ, then ϕ is isotropic if and only if ψ is isotropic.*

3.2 Central simple algebras and Brauer groups

Definition 3.2.0.1 (quaternion algebras)**.** *For a field F of characteristic not 2, and elements $a, b \in F^*$, define the associative algebra $(a, b)_{-1}$ to be the algebra generated by elements u, v with the relations $u^2 = a, v^2 = b, uv = -vu$.*

Exercise 3.2.0.2. *Show that $(a, b)_{-1}$ is a division algebra if and only if the form $\langle\langle a, b \rangle\rangle$ is anisotropic.*

Exercise 3.2.0.3 (not so easy without ingenuity)**.** *Show that if $(a, b)_{-1}$ is not division then it is isomorphic to $M_2(F)$.*

3.3 Galois cohomology

Suppose H is a functor from fields to torsion Abelian groups. For E/F, denote the map $H(F) \to H(E)$ by $res_{E/F}$, and suppose we also have maps $cor_{E/F} : H(E) \to H(F)$ such that $cor_{E/F} res_{E/F}$ is multiplication by $[E : F]$ when E/F is a finite extension.

As with Galois cohomology, for $\alpha \in H(F)$, define $ind(\alpha) = gcd\{[E : F] \mid res_{E/F}\alpha = 0\}$ and let $per(\alpha)$ be the order of α in $H(F)$.

Exercise 3.3.0.1. *Show that if $H(\overline{F}) = 0$ for $\overline{F}$ an algebraically closed field, that $per(\alpha)|ind(\alpha)$ for $\alpha \in H(F)$ and that $per(\alpha)$ and $ind(\alpha)$ have the same prime divisors.*

Recall that $ssd_\ell^{n,m}(F)$ is the minimum d such that $ind(\alpha)|per(\alpha)^d$ for any $\alpha \in H^n(E, \mu_\ell^{\otimes m})$ where E/F is any finite extension.

Exercise 3.3.0.2. *Show that $ssd_{\ell_1\ell_2}^{n,m}(F)$ is the max of $ssd_{\ell_i}^{n,m}(F)$ for $i = 1, 2$ if $(\ell_1, \ell_2) = 1$.*

Exercise 3.3.0.3. *Show that $ssd_p^{n,m}(F)$ is independent of m if p is prime.*

Exercise 3.3.0.4. *Show that $ssd_{p^n}^{n,m}(F) \leq ssd_p^{n,m}(F)$.*

Bibliography