Field Arithemtic Notes

Daniel Krashen

January 19, 2017

Contents

Chapter 1

Philosophy

Fields are important due to their ubiquity. While they arise in a number of different contexts in different branches of mathematics, field theory gives us a coherent set of tools in which to view structural properties.

It is fair to say that field theory is very much a work in progress. While the arithmetic of the rational numbers and number fields more generally, is a rich and exciting field, using a broad spectrum of techniques from algebra, analysis, and even topology, the study of more general fields raises many questions of a more foundational nature, as we try to generalize many strategies and concepts which one can take for granted in the case of number fields. The primary source for fields are

1. function fields of varieties
2. finitely generated fields, coming from number theory
3. fields of meromorphic functions on analytic manifolds

In addition, a rich source of (slightly more technical) examples, are fields constructed by taking inductive limits of other fields. Such constructions play an important role in producing counterexamples, and in intermediate steps in arguments – often, and somewhat counterintuitively, fields may become structurally simpler as they get larger (consider $\mathbb{C}$ versus $\mathbb{Q}$).

For various classes of fields, some examples of fundamental questions which would like to understand are as follows (followed by some names of formal ideas we will use to address them):

- what geometric/topological notions of "size" or "closeness" make sense?

  (**valuations and completions**)

- what notions of dimension do we have?

  (**cohomological dimension, Diophantine dimension, Brauer dimension, transcendence degrees, p-bases, ...**)

- can we make sense of positivity? How many ways can we make sense of this notion?

  (**real orderings and the Harrison topology**)

- what kinds of structural constraints do Galois groups have?

  (**the inverse Galois problem**)

- To what extent can we concretely describe how Galois extensions are constructed (for example, with a given group G)? What about other specific types of field extensions?

  (**generic Galois theory**)

- When can we interpret elements of fields as (rational) functions on a variety/space?

  (**Grothendieck's Anabelian conjectures**)

From another perspective, a very important tool in studying a field, is to consider the behaviour of algebraic objects over that field, such as algebras, quadratic forms, algebraic varieties, etcetera. The behaviour of such objects tells us a great deal about what the arithmetic of the field is like. Philosophically, one can think of the utility of this point of view in the following way: as mathematicians, a basic starting point is to ask the question "given a collection of polynomial equations, with coefficients in my field F, can I find a solution in F?" Which equations do and which equations don't have solutions represents a crucial kind of information about the field. As evidence for this, consider that the foundational notion of a field extension is based on the procedure of formally adjoining a solution to a single polynomial equation in one variable. On the other hand, there are a great deal of polynomials equations in the world, and if we consider arbitrary collections of such things, it is (in my own opinion) a bit too much for our limited minds to handle. For this reason, it makes sense to consider systems of equations for which we can assign strong conceptual meaning to their solutions. A source for such systems of equations of primary importance turns out to be algebraic objects: for example we might consider a system of equations for which a solution represents a zerodivisor in an algebra, an ideal in an algebra, or a subspace of a vector space on which some quadratic form vanishes.

A huge benefit of this perspective is the fact that these algebraic structures come with new rich sets of tools which can therefore be leveraged to understand the field's arithmetic. That is to say, by reinterpreting various problems in field arithmetic in terms of algebraic structures, we are able to leverage our understanding of these algebraic structures to get new information. We will see various examples of this: certain noncommutative algebras will give us ways to discuss relations between cyclic extensions, and quadratic forms will give us a perspective on a surprisingly wide array of arithmetic questions.

Further, as we will see later, the Galois cohomology groups (which play a role for a field which is in some sense analogous to the singular cohomology groups of a topological space) give rise to a rich collection of both field invariants, as well as invariants of algebraic structures. This additional connection has been crucial in recent developments in field theory, most notably in the proof of the Milnor conjecture by Voevodsky, as well as the establishmenent of the Norm Residue Isomorphism Theorem (the Bloch-Kato conjecture) by Voevodsky, Rost, Weibel, Suslin, Joukhovitski, and others.

From a related perspective, instead of looking at systems of equations whose solutions have these natural interpretation, one might also consider systems of equations that are at least simple to write down. The most obvious of these are those given by a single homogeneous polynomial. The study of when these have nontrivial solutions is the topic of Tsen-Lang theory, of the so-called C_i-property, and is encapsulated in the notion of "Diophantine Dimension."

The object of these notes is to give, after a brief refresher of field theory, a guide to these topics, with a particular eye towards Galois cohomology.

Chapter 2

Basics

2.1 Some useful algebraic structures

Definition 2.1.1. *Monoid*

Definition 2.1.2. *Cancellative Monoid*

Definition 2.1.3. *Group*

Definition 2.1.4. *Ring*

Definition 2.1.5. *Commutative Integral Domain*

Definition 2.1.6. *Field*

2.2 Fields

Definition 2.2.1. *A prime field is a field which contains no proper subfields.*

Proposition 2.2.2. *The only prime fields are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p a prime number, and $\mathbb{Q}$.*

Proof. Consider the (unique) homomorphism $\mathbb{Z} \to F$. □

Definition 2.2.3. *The characteristic of a field is nonnegative generator of the kernel of the map $\mathbb{Z} \to F$.*

Definition 2.2.4. *If F is a subfield of L, we say that L is a field extension of F and write L/F.*

Definition 2.2.5. *Simple extension*

Definition 2.2.6. *Splitting field*

Lemma 2.2.7. *Dedekind Lemma and corollary*

Definition 2.2.8. *Normality (= splitting field)*

Definition 2.2.9. *separability (and derivatives)*

Definition 2.2.10. *Galois extensions:*

- *normal + separable*
- *num auts = degree*
- $(E, G, 1)$ *iso to* $Hom_F(E, E)$

Theorem 2.2.11. *Galois correspondence*

2.3 Infinite things

Definition 2.3.1. *Inductive limits = direct limits ⊂ colimits*

Definition 2.3.2. *inverse limits = projective limits ⊂ limits*

Inverse limits come with natural "topologies" in many situations.
Direct limits can inheret topologies.

2.4 Tensor producs

Definition 2.4.1. *Let* V *and* W *be* F*-vector spaces. The tensor product* $V \otimes W = V \otimes_F W$ *is the vector space generated by all symbols of the form* $v \otimes w$*, subject to the relations*

1. $\lambda(v \otimes w) = \lambda v \otimes w = v \otimes \lambda w$ *for* $\lambda \in F$, $v, w \in V$
2. $(v + v') \otimes w = v \otimes w + v' \otimes w$ *for* $v, v', w \in V$
3. $v \otimes (w + w') = v \otimes w + v \otimes w'$ *for* $v, w, w' \in V$

Proposition 2.4.2. *Suppose that* V *and* W *are vector spaces with bases* $\{v_i\}_{i \in I}$ *and* $\{w_j\}_{j \in J}$ *respectively. Then* $V \otimes_F W$ *has a basis given by* $\{v_i \otimes w_j\}_{(i,j) \in I \times J}$*. In particular, if* V *and* W *are finite dimensional, then* $\dim_F(V \otimes_F W) = (\dim_F V)(\dim_F W)$.

Proof. Consider the maps $f_k : V \otimes W \to W$ and $g_\ell : V \otimes W \to V$ given by

$$f_k(\sum_{i,j} v_i \otimes w_j) = \sum$$

□

Definition 2.4.3. *Let* F *be a field. An (associative, unital)* F*-algebra is a* F*-vector space* A*, together with a multiplication* A