M.A. Lopuhaä

Field Topologies on Algebraic Extensions of Finite Fields

Bachelorscriptie, 24 juni 2011
Scriptiebegeleiders: dr. K.P. Hart, prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden
Contents

1 Introduction 1

2 Approximations of local bases 3
   2.1 Definitions 3
   2.2 Expanding approximations 4
   2.3 Making topologies 5

3 Topologies with continuous automorphisms 9
   3.1 Definition and basic properties 9
   3.2 Expanding approximations 10

4 A field topology with nontrivial subfield topologies 13

Bibliography 14
Chapter 1

Introduction

Definition 1.1.1. Let $K$ be a field, and $\mathcal{T}$ a topology on $K$. We call $\mathcal{T}$ a field topology if the maps

\begin{align*}
K \times K &\to K : (x, y) \mapsto x + y, \\
K \times K &\to K : (x, y) \mapsto x \cdot y, \\
K^* &\to K^* : x \mapsto x^{-1},
\end{align*}

are continuous, in which $K \times K$ is given the product topology and $K^*$ the subspace topology.

In this thesis, we will be using methods developed by Podewski [1] to prove that any infinite countable field $F$ admits exactly $2^{2^{\aleph_0}}$ field topologies. In the case of an algebraic closure of a finite field $\mathbb{F}_q$, we can ensure that all automorphisms are continuous with respect to these topologies. Furthermore, we will show that there exists a field topology on this algebraic closure such that the subspace topology on every infinite subfield is neither discrete nor antidiscrete. This raises the question whether such a topology exists such that all automorphisms are continuous as well.
CHAPTER 1. INTRODUCTION
Chapter 2

Approximations of local bases

This section largely reviews material from [1].

2.1 Definitions

Definition 2.1.1. Let $K$ be a countably infinite field. Consider the following functions:

- $\zeta : \mathcal{P}(K) \to \mathcal{P}(K) : X \mapsto X - X = \{x - y : x, y \in X\}$;
- $\eta : \mathcal{P}(K) \to \mathcal{P}(K) : X \mapsto X \cdot X$;
- $\theta : \mathcal{P}(K) \to \mathcal{P}(K) : X \mapsto \frac{X}{X \setminus \{1\}}$;
- $\xi_A : \mathcal{P}(K) \to \mathcal{P}(K) : X \mapsto A \cdot X$, one for every $A \subset K^*$.

A family in $K$ is a subset $A$ of $[K]^{<\omega}$ such that every $a \in K$ is in some $A \in A$, and for all $A, B \in A$, the sets $A \cup B, \xi_B(A)$ and $\phi(A)$ are also in $K$, for all $\phi \in \{\zeta, \eta, \theta\}$. Given a family $A$ in $K$, as $A$ is countably infinite, we can choose a sequence $(\phi_n)_{n \in \omega}$ in $\{\zeta, \eta, \theta\} \cup \{\xi_A : A \in A\}$ such that every element occurs infinitely often (we employ the set-theoretic notation $\omega = \mathbb{Z}_{\geq 0}$). Occasionally, we will extend $\phi_n$ to a function $\phi_n : \mathcal{P}(K(X_1, \ldots, X_l)) \to \mathcal{P}(K(X_1, \ldots, X_l))$, for some integer $l$. We denote $d(n) = |\{k \leq n : \phi_k \in \{\zeta, \eta, \theta\}\}|$.

Example 2.1.2. For any field $K$, the collection of finite subsets of $K$ is a family in $K$. Also, if $K \subseteq L$ is an extension and $A$ is a family in $L$, then $\{A \cap K : A \in A\}$ is a family in $K$.

Lemma 2.1.3. Let $(V_n)_{n \in \omega}$ be a sequence of subsets of $K$ such that, for every $n \in \omega$:

- $0 \in V_n$;
- $1 \notin V_n$;
- $V_{n+1} \subset V_n$;
- $\phi_n(V_{n+1}) \subset V_n$.

Then $\{x + V_n : x \in K, n \in \omega\}$ is the base for a field topology on $K$.

We omit the straightforward proof.

Definition 2.1.4. An approximation of a local base at $0$, or briefly an approximation, is a function $f : \omega \cup \{-1\} \to [K]^{<\omega}$ (the set of finite subsets of $K$) such that the following conditions are satisfied:

1. $0 \in f(n)$ for all $n \in \omega$;
2. $1 \in f(-1)$;
3. \( f(n) \cap f(-1) = \emptyset \) for all \( n \in \omega \);
4. \( f(n + 1) \subset f(n) \) for all \( n \in \omega \);
5. \( \phi_n(f(n + 1)) \subset f(n) \) for all \( n \in \omega \).

The set of all approximations is denoted \( \mathcal{P} \). The set of all approximations whose image is in a given family \( \mathcal{A} \) is denoted \( \mathcal{P}_\mathcal{A} \).

For two approximations \( f \) and \( f' \) we define \( f' \leq f \) if \( f'(n) \subset f(n) \) for every \( n \in \omega \cup \{-1\} \); this defines a partial order on \( \mathcal{P} \).

**Lemma 2.1.5.** Let \( C \) be a chain in \( \mathcal{P} \), and for \( n \in \omega \), define \( V_n^C = \bigcup_{f \in C} f(n) \). Then
\[
\{ x + V_n^C : x \in K, n \in \omega \}
\]
is the basis of a field topology on \( K \).

Again, the proof is fairly straightforward, so we omit it.

### 2.2 Expanding approximations

In this section, we describe the conditions under which approximations may be expanded in a way that will suit us in the coming sections.

**Theorem 2.2.1.** Let \( K \subset L \) be two fields, with \( \mathcal{A} \) and \( (\phi_k)_{k \in \omega} \) defined in \( L \). Let \( f \in \mathcal{P}_{(A,A \in \mathcal{A}, A \subset K)} \)
and let \( n \in \omega \cup \{-1\} \), such that \( \phi_k \in \{\zeta, \eta, \theta\} \cup \{\xi_A : A \in \mathcal{A}, A \subset K\} \) for \( k < n \). Then there exist \( l \in \omega \) and a finite set \( G \subset K[X_1, \ldots, X_l] \) such that
\[
\phi_{\xi_A}(f(n + 1)) \subset f(n) \quad \text{for all finite subset } A \in \mathcal{A}
\]
for every \( n \in \omega \) such that \( f(n) \neq \emptyset \) and \( f(m) = f'(m) \) for all \( m > n \) and for \( m = -1 \) if \( n \neq -1 \).

2. none of the polynomials in \( G \) has a zero in \( A \).

Furthermore, if \( n \in \omega \), then \( l \) and \( G \) can be chosen to be such that \( l \leq 2d(n) \) and every \( g \in G \) is of degree \( \leq 2d(n) \).

**Proof.** For \( n = -1 \), given \( f \), let \( l = 1 \) and \( G = \{ X_1 - \alpha : \alpha \in f(0) \} \in K[X_1] \). Then every function as in 1 must satisfy \( f'' \geq f'' \), where the function \( f'' : \omega \cup \{-1\} \rightarrow [L[^\omega] \subseteq L \) given by
\[
f''(m) := \begin{cases} f(-1) \cup A, & \text{if } m = -1; \\ f(m), & \text{else.}\end{cases}
\]

Then \( f(-1) \cup A \in \mathcal{A} \), so \( f'' \in \mathcal{P}_\mathcal{A} \) if and only if \( A \cap f(0) = \emptyset \), which is true if and only if \( g \) has no zeroes in \( A \).

For \( n \in \omega \) we use induction on \( n \) to prove the stronger statement that \( G \) and \( l \) can be found with the properties in the lemma such that \( X_i - 1 \in G \) for all \( 1 \leq i \leq l \). The proof for \( n = 0 \) is the same to that of \( n = -1 \), using \( l = 1 \) and \( G = \{ X_1 - \alpha : \alpha \in f(-1) \}; \) then \( l = 1 \leq 2d(0) = 1 \), and \( X_1 - 1 \in G \). Now assume the theorem holds for \( n \), and let \( l \in \omega \) be an integer and \( G \) a set of polynomials, satisfying the conditions of the theorem. We find a \( l' \) and \( G' \) that work for \( n + 1 \).

If \( \phi_n = \xi_B \) for some \( B \subset K \), then look at the set
\[
G' = \{ g(h_0, \ldots, h_l) : g \in G, h_i \in \{X_i\} \cup f(n + 1) \cup \xi_B((X_i \cup f(n + 1))) \subset K[X_1, \ldots, X_{2l}] \}.
\]

Then by the induction hypothesis, \( l \leq 2d(n) = 2^{d(n + 1)} \), and every polynomial in \( G' \) is of degree at most \( 2d(n) = 2^{d(n + 1)} \); furthermore, for all \( 1 \leq i \leq l \), \( X_i - 1 \in G \subset G' \). Note that for a set \( A \in \mathcal{A} \), no polynomial in \( G' \) has a zero in \( A \) if and only if no polynomial in \( G \) has a zero in \( (A \cup f(n + 1) \cup \xi_B(A \cup f(n + 1))) \).
2.3. MAKING TOPOLOGIES

If \( \phi_n = \zeta \) or \( \phi_n = \eta \), then we take

\[ G' = \{ g(h_1, \ldots, h_l) : g \in G, h_i \in \{ X_{2i-1}, X_{2i} \} \cup f(n+1) \cup \phi_n(\{ X_{2i-1}, X_{2i} \} \cup f(n+1)) \}. \]

Note that \( G' \) is a subset of \( K[X_1, \ldots, X_{2l}] \), and that here we have polynomials in \( 2l \leq 2^{d(n)+1} = 2^{d(n+1)} \) variables of degree at most \( 2l \). Also, it is easy to see that for all \( 1 \leq i \leq 2l \), the polynomial \( X_i - 1 \) is in \( G' \). Again, for a set \( A \subset K \), no polynomial in \( G' \) has a zero in \( A' \) if and only if no polynomial in \( G \) has a zero in \( (A \cup f(n+1))' \).

If \( \phi_n = \theta \), then define

\[ G'' = \{ g(h_1, \ldots, h_l) : g \in G, h_i \in \{ X_{2i-1}, X_{2i} \} \cup f(n+1) \cup \theta(\{ X_{2i-1}, X_{2i} \} \cup f(n+1)) \}. \]

Note that \( G'' \) is a subset of \( K(X_1, \ldots, X_{2l}) \). If we write the elements of \( G'' \) in the form \( j/h \), with \( j, h \in K[X_1, \ldots, X_{2l}] \) without common factors, we take \( G'' = \{ j : \exists h \in K[X_1, \ldots, X_{2l}] \text{ such that } j/h \in G'' \text{ and } \gcd(j, h) = 1 \} \). We will show that for every \( (a_1, \ldots, a_2l) \in K^{2l} \), one has \( j(a_1, \ldots, a_2l) = 0 \) for some \( j \in G'' \) if and only if there is some \( g \in G'' \) such that \( g(a_1, \ldots, a_2l) \) is defined and equal to \( 0 \). The ‘if’ part of the statement is obvious; as for the ‘only if’ part, if \( j \in G'' \) and \( j(a_1, \ldots, a_2l) = 0 \), and \( h \) is such that \( j/h \in G'' \) and \( \gcd(j, h) = 1 \), then either \( h(a_1, \ldots, a_2l) = 0 \), or \( (j/h)(a_1, \ldots, a_2l) = 0 \) is defined and equal to \( 0 \). If we write \( j/h = g(h_1, \ldots, h_2l) \) for some \( g \in G'' \) and \( h(a_1, \ldots, a_2l) = 0 \), then some \( h_l(a_1, \ldots, a_2l) \) must be undefined. This is possible only if \( h_l = \theta(X_{2l-1}, X_{2l}) = \frac{X_{2l-1}}{X_{2l}} \) for some \( x \in f(n+1) \). Either way, \( a_2l \) must be equal to \( 1 \). As \( X_i - 1 \in G \), our construction ensures that \( X_{2l-1} - 1 \in G' \), so \( (a_1, \ldots, a_2l) \) is a zero of the defined \( X_{2l-1} - 1 \in G' \). Note that here we have polynomials in \( 2l \leq 2^{d(n)+1} = 2^{d(n+1)} \) variables of degree at most \( 2l \).

Now we will show that for the set \( G' \), the statements 1 and 2 are equivalent. Let \( A \subset \mathcal{A} \) be such that no function in \( G' \) has a zero in \( A' \); hence no polynomial in \( G \) has any zeroes in \( (A \cup f(n+1))' \). Since this set is in \( \mathcal{A} \), by the induction hypothesis there exists an approximation \( f'' \in \mathcal{P}_A \) such that \( f'' \geq f \) and \( A \cup f(n+1) \cup \phi_n(A \cup f(n+1)) \subset f''(n) \), and \( f(m) = f''(m) \) for all \( m > n \) and for \( m = -1 \). Now consider the function \( f' : \omega \cup \{-1\} \rightarrow \mathcal{A} \) given by

\[ f'(m) := \begin{cases} f''(n+1) \cup A, & \text{if } m = n+1; \\ f''(m), & \text{otherwise.} \end{cases} \]

This is an approximation in \( \mathcal{P}_A \) which satisfies \( A \subset f'(n+1) \) and \( f(m) = f'(m) \) for all \( m > n+1 \) and for \( m = -1 \).

Now let \( A \subset \mathcal{A} \) be finite such that there exists an approximation \( f' \in \mathcal{P}_A \) such that \( f \leq f' \) and \( A \subset f'(n+1) \) and \( f'(m) = f(m) \) for all \( m > n \) and for \( m = -1 \). Consider the function \( f'' : \omega \cup \{-1\} \rightarrow \mathcal{A} \) given by

\[ f''(m) := \begin{cases} f(n+1), & \text{if } m = n+1; \\ f'(m), & \text{otherwise.} \end{cases} \]

This is an approximation which satisfies \( A \cup f(n+1) \cup \phi_n(A \cup f(n+1)) \subset f''(n) \), and \( f''(m) = f(m) \) for all \( m > n+1 \) and for \( m = -1 \). By the induction hypothesis no polynomial in \( G \) has any zeroes in \( (A \cup f(n+1))' \); but this means precisely that no polynomial in \( G' \) has any zeroes in \( A' \).

**Corollary 2.2.2.** Let \( f, n, G \) be as in the previous theorem. If \( \{0\} \in \mathcal{A} \), then for all \( g \in G \), the value \( g(0, \ldots, 0) \) is unequal to \( 0 \).

**Proof.** This follows from the previous theorem and the fact that there is an approximation \( f' \) satisfying 1 of the previous theorem for \( A = \{0\} \), namely \( f' = f \).

**2.3 Making topologies**

**Lemma 2.3.1.** Using the family \( \mathcal{A} = [K]^{<\infty} \), let \( f \) be an approximation in \( K \), and let \( n \in \omega \cup \{-1\} \). Then for almost all \( r \in K \) (that is, for all \( r \in K \) except for a finite subset), there exists an approximation \( f' \geq f \) such that \( r \in f'(n) \) and \( f(m) = f'(m) \) for all \( m > n \) and for \( m = -1 \) if \( n \neq -1 \).
Proof. By theorem 2.2.1, using \( L = K \), there exists a finite set of polynomials \( G \subseteq K[X_1, \ldots, X_1] \) such that there exists an approximation \( f' \) satisfying the theorem if and only if for all \( g \in G \), \( g \) has no zero in \( \{ r \}^1 \). This is true if and only if \( g(r, r, \ldots, r) \neq 0 \) for all \( g \in G \). Because \( \{ 0 \} \in \mathcal{A} \), one has \( g(0, \ldots, 0) \neq 0 \), one has \( g(X, \ldots, X) \neq 0 \), and hence every \( g(X, \ldots, X) \) has only a finite number of zeroes. \( \square \)

Now we can use the approximations to make field topologies on \( K \). We regard every nonnegative integer as the set of its predecessors: \( n = \{ 0, 1, \ldots, n - 1 \} \). Furthermore, for two sets \( A \) and \( B \) we use the notation \( \uparrow B \) for the set of functions from \( A \) to \( B \), and \( ^{<\omega}A = \bigcup_{n \in \omega}n\cdot A \). For every \( s \in ^{<\omega}2 \) we recursively define an approximation \( f^s \) such that for every \( n \geq 1 \) and \( s \in ^n2 \),

\[
f^{s|n-1} \leq f^s,
\]

where \( s \upharpoonright n - 1 \) denotes the restriction of \( s \) to \( n - 1 = \{ 0, 1, \ldots, n - 2 \} \), and

\[
f^s(-1) \cap \bigcap_{t \in ^n2 \setminus \{s\}} f^t(n) \neq \emptyset.
\]

(2.3.2)

For \( \emptyset \), the unique element of \( ^02 \), we define \( f^\emptyset : \omega \cup \{-1\} \to [K]^{<\omega} \) by

\[
f^\emptyset(m) = \begin{cases} 
\{1\}, & \text{if } m = -1; \\
\{0\}, & \text{otherwise.}
\end{cases}
\]

Now let \( n > 0 \), and assume we have defined \( f^s \) for all \( s \in ^{n-1}2 \). Let \( \{ s_1, \ldots, s_{2^n} \} \) be an ordering of \( ^n2 \). Because of lemma 2.3.1 there exists an element \( \alpha \in K \) such that for every \( k \leq 2^n \) there exist \( f^s_k \in \mathfrak{P} \) such that

\[
f^{s_k|n-1} \leq f^{s_k}_1 \text{ for all } k \leq 2^n
\]

(2.3.3)

and

\[
\alpha \in f^{s_k}_1(-1) \cap \bigcap_{2 \leq k \leq 2^n} f^{s_k}_1(n).
\]

Now analogously define recursively for every \( 2 \leq m \leq 2^n \), for every \( k \leq 2^n \) a function \( f^{s_k}_m \in \mathfrak{P} \) such that

\[
f^{s_k}_{m-1} \leq f^{s_k}_m \text{ for all } k \leq 2^n
\]

and

\[
f^{s_k}_k(-1) \cap \bigcap_{h \neq k} f^{s_k}_h(n) \neq \emptyset.
\]

Take \( f^{s_k} = f^{s_k}_{2^n} \); then \( f^s \) satisfies (2.3.2) for every \( s \in ^n2 \). For \( x \in ^{<\omega}2 \), define \( C_x = \{ f^x|n : n \in \omega \} \). This is a chain of approximations, and hence defines a field topology \( T_x \) on \( K \). For a subset \( X \subseteq ^{<\omega}2 \), define the field topology \( T_X = \bigvee_{x \in X} T_x \), the coarsest topology such that all the open sets of all the \( T_x \) are open; this is again a field topology. In any topology such that all the sets of \( T_g \) are open for all \( g \in X \), finite intersections of open sets from different \( T_g \) are also open. Therefore, \( T_X \) is the topology generated by elements of the form \( \bigcap_{i=1}^n U_i \), with \( n \) some integer and every \( U_i \) open in some \( T_y \). Since the collection of these sets is closed under intersection, these elements actually constitute a basis of \( T_X \).

Lemma 2.3.4. Let \( X, Y \subseteq ^{<\omega}2 \) be different. Then \( T_X \neq T_Y \).

Proof. Without loss of generality we may assume that we can choose \( h \in X \setminus Y \). Using the notation of 2.1.3, \( V_0^{<h} \cap V_1^{<h} \) is empty, so one has \( 0 \notin V_1^{<h} \) in \( T_X \). A basis element of \( T_Y \) is of the form
$\bigcap_{i=1}^{m} g_i(n_i)$, with $n_i \in \omega$ and $g_i \in Y$. Let $n \in \omega$ be such that $n \geq n_i$ for all $i$ and such that $h \upharpoonright n$ differs from all $g_i \upharpoonright n$. Then

$$
\emptyset \subseteq f^{h\upharpoonright n}(1) \cap \bigcap_{i=1}^{m} f^{g_i\upharpoonright n}(n)
\subseteq f^{h\upharpoonright n}(1) \cap \bigcap_{i=1}^{m} f^{g_i\upharpoonright n}(n_i)
\subseteq V_{-1}^{C_h} \cap \bigcap_{i=1}^{m} V_{n_i}^{C_{g_i}}.
$$

This implies that $0 \in V_{-1}^{C_h}$ in $\mathcal{T}_Y$, and hence $\mathcal{T}_X \neq \mathcal{T}_Y$. 

**Theorem 2.3.5.** Let $K$ be a countable field. Then there exist exactly $2^{2^{\aleph_0}}$ field topologies on $K$.

**Proof.** By lemma 2.3.4, there exist at least $2^{2^{\aleph_0}}$ field topologies on $K$. Because a topology is a set of subsets of $K$, this is also the maximum number. 

\qed
Chapter 3

Topologies with continuous automorphisms

3.1 Definition and basic properties

**Definition 3.1.1.** Let $K$ be an algebraic extension of a countable field $F$, and $A$ a subset of $K$. We call $A$ stable under $\text{Aut}_F(K)$ if $\sigma[A] \subset A$ for every $\sigma \in \text{Aut}_F(K)$. If $f$ is an approximation, then $f$ is said to be stable under $\text{Aut}_F(K)$ if $f(n)$ is stable under $\text{Aut}_F(K)$ for every $n \in \omega \cup \{-1\}$.

The reason for looking at these approximations is stated without proof in the following lemma.

**Lemma 3.1.2.** Let $C$ be a chain of approximations that are stable under $\text{Aut}_F(K)$. Then the action $\text{Aut}_F(K) \times K \to K : (\sigma, x) \mapsto \sigma(x)$ is continuous, where $\text{Aut}_F(K)$ is given the Krull topology (see [2], p21) and $K$ the topology induced by $C$.

Again, we omit the simple proof.

**Definition 3.1.3.** Let $F_q$ be a finite field, and let $\alpha \in \overline{F_q}$, an algebraic closure of $F_q$. The degree of $\alpha$ is defined by

$$\deg \alpha = [F_q(\alpha) : F_q].$$

Note that this is equal to $\min\{n \in \omega : \alpha \in F_q^n\}$, see [2], p98.

**Lemma 3.1.4.** Let $x_n = \#\{\alpha \in F_q^n : \deg \alpha = n\}$. Then

$$\lim_{n \to \infty} \frac{x_n}{q^n} = 1.$$

**Proof.** Because $F_q^n$ has, by definition, $q^n$ elements, we have $x_n \leq q^n$. Furthermore, $\sum_{d|n} x_d = q^n$. Therefore,

$$x_n = q^n - \sum_{d|n, d<n} x_d \geq q^n - \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = q^n - \frac{q - 1}{q - 1}\left(q^{\lfloor \frac{n}{2} \rfloor} - 1\right),$$

from which the lemma follows easily. $\square$
Lemma 3.1.5. Let $K$ be an infinite algebraic extension of a finite field $F$, and $A$ the family in $K$ consisting of all finite subsets of $K$ stable under $\text{Aut}_F(K)$. Given $A$, let $(\phi_n)_{n \in \omega}$ be a sequence as in Definition 2.1.1, and $f$ an approximation stable under $\text{Aut}_F(K)$, and $n \in \omega \cup \{-1\}$. Then there exists $l \in \omega$ and a finite $G \subset F[X_1, \ldots, X_l]$ such that for every $A \in A$, the following statements are equivalent:

- There exists an approximation $f' \geq f$ such that $f'$ is stable under $\text{Aut}_{F_q}(K)$, $A \subset f'(n)$, and $f(m) = f'(m)$ for all $m > n$ and for $m = -1$ if $n \neq -1$.

- For every $g \in G$, the polynomial $g$ has no zeroes in $A'$.

Proof. By Theorem 2.2.1 there exist $l \in \omega$ and $G \subset K[X_1, \ldots, X_l]$ such that for every $A \in A$:

1. There exists an approximation $f' \geq f$ such that $f'$ is stable under $\text{Aut}_F(K)$, $A \subset f'(n)$, and $f(m) = f'(m)$ for all $m > n$ and for $m = -1$ if $n \neq -1$.

2. Every $g' \in G'$ has no zeroes in $A'$.

Let $G = \{g : g$ is the product of the conjugates of $g'$ for some $g' \in G'\}$. Then, because $A$ is closed under $\text{Aut}_{F_q}(K)$, some $g \in G$ has a zero in $A'$ if and only if there is some $g' \in G'$ with a zero in $A'$; this proves our lemma. 

\[\blacksquare\]

3.2 Expanding approximations

Lemma 3.2.1. Let $t$ and $n$ be integers greater than or equal to 2, and $G$ be the directed graph having the set $Z/nZ$ as vertices and $\{(k, k+1) : k \in Z/nZ\}$ as edges, and let $a_1, \ldots, a_t \in Z/nZ$. Then there is a $k \in A = \{a_1, \ldots, a_t\}$ such that the distance in $G$ from $k$ to any other point in $A$ is at most $\lfloor \frac{t-1}{n} \rfloor$.

Proof. Note that for $a,b \in Z/nZ$, the distance from $a$ to $b$ is $|b-a|$, where $|x|$ denotes $x$ considered modulo $n$ and taken between 0 and $n-1$. Let $a_1', a_2', \ldots, a_t'$ be an enumeration of the $a_i$ in ascending order (from 0 to $n-1$), and $a_i' + 1 = a_i', a_i' + 1 = a_i$ for $i \leq t - 1$, and $f_i = a_i' - a_i'$. Then $f_i$ sum to $n$, so there must be some $m$ such that $f_m \geq \lfloor \frac{t-1}{n} \rfloor$. For this $m$ we have $[a_i'-a_m]+1, \ldots, [a_i'-a_m+1] \leq \lfloor \frac{t-1}{n} \rfloor$; to see this, note that $[a_i'-a_m]+1 = n + a_i'-a_m+1 \leq n + a_i'-a_m+1 \leq \lfloor \frac{t-1}{n} \rfloor$ for $j \leq m$, and for $j > m$, it holds that $[a_i'-a_m+1] = a_i'-a_m+1 = \sum_{i=m+1}^{t} f_i \leq n - f_m \leq \lfloor \frac{t-1}{n} \rfloor$, as the $f_i$ are nonnegative. Hence $a_i'+1$ satisfies the conditions of the lemma. 

\[\blacksquare\]

Theorem 3.2.2. Let $K$ be an infinite algebraic extension of a finite field $F_q$, and let $f$ be an approximation stable under $\text{Aut}_{F_q}(K)$, and $m \in \omega \cup \{-1\}$. Let $x_n$ be as in lemma 3.1.4, and for $n \in Z\geq0$ such that $F_{q^n} \subset K$, let $B_n$ be the set of $\alpha \in K$ such that deg $\alpha = n$ and there exists $f' \in F$ stable under $\text{Aut}_{F_q}(K)$ such that $f' \geq f$, $\alpha \in f'(m)$ and $f'(k) = f(k)$ for $k > m$ or $k = -1$ if $m \neq -1$. Then $\lim_{n \to \infty} \frac{B_n}{x_n} = 1$, where $n$ ranges over the integers such that $F_{q^n} \subset K$.

Proof. For $\alpha \in K$, the set of conjugates of $\alpha$ is the set $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{deg_{\alpha} - 1}}\}$ (see [2], p25). By lemma 3.1.5, there exists a finite set of polynomials $G \subset F_q[X_1, \ldots, X_l]$ such that there exists an approximation $f'$ satisfying the above conditions if and only if no $g \in G$ has any zeroes in $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{deg_{\alpha} - 1}}\}$; let $k = \prod_{g \in G} g$. For $\alpha$ of a fixed degree $n$, this implies that such an approximation exists if and only if $\alpha$ is not a zero of any polynomial of the form $k(X^{q^{e_1}}, X^{q^{e_2}}, \ldots, X^{q^{e_l}})$, where $0 \leq e_1, \ldots, e_l < n$. By Lemma 3.2.1, there is an $e_m$ such that all the values $[e_i - e_m]$ are lesser than or equal to $\lfloor \frac{t-1}{n} \rfloor$. Now $\alpha^{q^{e_m}}$ is a zero of the polynomial 

$$k \left(X^{q^{e_1-e_m}}, X^{q^{e_2-e_m}}, \ldots, X^{q^{e_l-e_m}}\right) \in F_q[X].$$

Now $\alpha$ is a zero of this polynomial as well; hence, for every $x \in K$ of degree $n$, one has $x \in B_n$ if and only if there are no $0 \leq e_1, e_2, \ldots, e_l \leq \lfloor \frac{t-1}{n} \rfloor$ such that $x$ is a zero of $k(X^{q^{e_1}}, X^{q^{e_2}}, \ldots, X^{q^{e_l}})$. 

\[\blacksquare\]
3.2. EXPANDING APPROXIMATIONS

Because \(k(0, \ldots, 0) \neq 0\) by Corollary 2.2.2, polynomials of this form are not the zero polynomial, and of degree at most \(\deg(k) \cdot \max_i \{q^{e_i}\}\), so they cannot have more than \(\deg(k) \cdot \max_i \{q^{e_i}\}\) zeroes. This implies that

\[
|B_n| \geq q^n - \sum_{e_1=0}^{\lfloor \frac{l-1}{l} \cdot n \rfloor} \cdots \sum_{e_t=0}^{\lfloor \frac{l-1}{l} \cdot n \rfloor} \deg(k) \cdot \max_i \{q^{e_i}\}
\]

\[
\geq q^n - \left(\frac{l-1}{l} \cdot n + 1\right)^t \cdot q^{\lfloor \frac{l-1}{l} \cdot n \rfloor} \cdot \deg(k).
\]

Hence \(\lim_{n \to \infty} \frac{|B_n|}{x_n} = \lim_{n \to \infty} \frac{|B_n|}{q^n \cdot x_n} = 1\).

**Theorem 3.2.3.** Let \(F\) be a finite field, and let \(K\) be an infinite algebraic extension of \(F\). Then there exist \(2^{2^{\aleph_0}}\) field topologies on \(K\) such that the action of \(\text{Aut}_F(K)\) on \(K\) is continuous.

**Proof.** This can be proven similarly to theorem 2.3.5. Analogously, for every \(l \in <\omega_2\) we define an approximation \(f^l\) stable under \(\text{Aut}_F(K)\) such that (2.3.2) holds, starting with \(f^0: \omega \cup \{-1\} \to [K]^{<\omega}\) defined as in section 2.3. Because of theorem 3.2.2, we can expand the approximations. Now we can make topologies, which analogously to theorem 2.3.4 are all different. \(\Box\)
Chapter 4

A field topology with nontrivial subfield topologies

In this section, we refine the methods in section 2.3 to construct a Hausdorff field topology on an algebraic closure of a finite field $F$ such that for every infinite algebraic extension $F \subset L$, the induced topology on $L$ is not discrete. We start off with some definitions:

**Definition 4.1.1.** Let $F = F_q$ be a finite field, and $\overline{F}$ an algebraic closure of $F$. Then we define the following subfields of $\overline{F}$, where $p$ is a prime and $P$ an infinite set of primes:

\[
\begin{align*}
F_p &= \{ x \in \overline{F} : [F(x) : F] is a power of p \} \\
F_P &= \{ x \in \overline{F} : [F(x) : F] is squarefree, and its prime divisors are elements of P \} \\
F_{<p} &= \{ x \in \overline{F} : all primes dividing [F(x) : F] are smaller than p \}
\end{align*}
\]

To make this topology, we desire further constraints on $(\phi_n)_{n \in \omega}$: for $n \leq 2k - 3$, $\phi_n$ must be an element of $\{\zeta, \eta, \theta\} \cup \{\xi_A : A \subset F_{<p_k}, A \ finite\}$ (we use $A = [L]^{<\infty}$), where $p_i$ denotes the $i$-th prime. Furthermore, $2^{d(n)}$ must be smaller than $p_n$. Also, let $(q_i)_{i \in \omega}$ be a sequence of primes such that $q_i \leq p_i$ for all $i$, and every prime occurs in $(q_i)_{i \in \omega}$ an infinite number of times.

**Theorem 4.1.2.** Let $F$ be a finite field. Then there exists a field topology on $F$ such that for any infinite subfield $L \subset \overline{F}$ the induced topology is nontrivial, i.e., neither discrete nor antidiscrete.

For the proof of this theorem, we need two lemmas, which we will prove later on.

**Lemma 4.1.3.** Let $F = F_q$ be a finite field. Then for any infinite algebraic extension $F \subset L$, the field $L$ must contain a subfield either of the form $F_p$ for some prime $p$, or $F_P$ for some infinite set of primes $P$.

**Lemma 4.1.4.** There exists an increasing sequence of approximations $(f^n)_{n \in \omega}$ satisfying the following conditions:

- for every $k \geq 2$, the image of $f^{2k-2}$ is contained in $F_{<p_k}$;
- for every $k \geq 3$, the image of $f^{2k-3}$ is contained in $F_{<p_k}$;
- for every $n$ and every $m > n$, the set $f^n(m)$ is equal to $\{0\}$;
- for every $n$, the set $f^n(-1)$ is equal to $\{-1\}$;
- for every $k \geq 1$, the set $f^{2k}(2k)$ is of the form $\{x\}$ for some $x \in F_{q_i}$;
- for every $k \geq 1$, the set $f^{2k-1}(2k - 1)$ is of the form $\{x\}$ for some $x$ of degree $p_k$. 

13
Proof of Theorem 4.1.1 from 4.1.3 and 4.1.4. By Lemma 4.1.3, it is sufficient to construct a topology such that the induced topology on every $F_p$ and $F_P$ is nontrivial. This is true if and only if $0$ is not an isolated point in any of those fields and the topology is not antidiscrete. Take the field topology induced by the sequence $(f_n)_{n \in \omega}$ of Lemma 4.1.4. As our construction gives neighborhoods of $0$ not containing $1$, the topology will not be antidiscrete. For any prime $p$, elements of $F_p$ occur in $f^{2k}(2k)$ for arbitrarily large $k$, so $0$ will not be an isolated point in $F_p$. Also, for any infinite set of primes $P$, elements of $F_P$ occur in $f^{2k-1}(2k - 1)$ for arbitrarily large $k$, so $0$ will not be discrete in $F_P$; hence this topology is nontrivial on any infinite subfield of $F$.

Proof of Lemma 4.1.3. Define $A \subset \mathbb{Z}_{\geq 1}$ as $A = \{ n \in \mathbb{Z}_{\geq 1} : F_{q^n} \subset L \}$. Then $A$ is infinite and $L = \bigcup_{n \in A} F_{q^n}$. Furthermore, if $m$ and $n$ are elements of $A$, then so are any of their divisors, as well as their least common multiple. This means that $A$ is defined by the prime powers occurring in it. As $A$ is infinite, either an unlimited number of primes must occur in $A$, or arbitrarily large powers of a certain prime must occur in $A$; so $L$ either has a subfield of the form $F_P$ for a certain infinite set of primes $P$, or a subfield of the form $F_P$ for a certain prime $p$.

Proof of Lemma 4.1.4. We recursively define our approximations by setting $f^0 = f^0$ as defined in section 2.3; indeed the image of $f^0$ is contained $F_{<2} = F$. For $n = 2k$ given an approximation $f^{2k-1}$ satisfying the conditions in the lemma, we want to choose an approximation $f^{2k}$ such that:

- the image of $f^{2k}$ is contained in $F_{<p^{k+1}}$;
- $f^{2k-1} \leq f^{2k}$;
- $f^{2k-1}(m) = f^{2k}(m)$ for $m = -1$ and $m > 2k$;
- $f^{2k}(2k) = \{ x \}$ for some $x \in F_{q^k}$.

As $f^{2k-1}(m)$ equals $\{ 0 \}$ for all $m > 2k - 1$, condition 5 from 2.1.2 is implied by condition 1 for $n \geq 2k - 1$; hence for $n \geq 2k - 1$, we may assume without loss of generality that $\phi_n = \xi_0$ for those $n$; as $\phi_n \in \{ \zeta, \eta, \theta \} \cup \{ \xi_n : a \in F_{<p^{k+1}} \}$ for $n < 2k - 1$, we may assume that $\phi_n$ is defined within $F_{<p^{k+1}}$. As the image of $f^{2k-1}(m)$ is contained in $F_{<p^{k+1}}$, we may apply lemma 2.3.1 with $K = F_{<p^{k+1}}$, $f = f^{2k-1}$ and $n = 2k$. As $F_{q^k}$ is an infinite subfield of $F_{<p^{k+1}}$, there is an $x \in F_{q^k}$ such that $f^{2k}$ satisfies the above conditions.

For $n = 2k - 1$, given $f^{2k-2}$ satisfying the conditions in the lemma, we wish to make $f^{2k-1}$ such that:

- the image of $f^{2k-1}$ is contained in $F_{<p^{k+1}}$;
- $f^{2k-2} \leq f^{2k-1}$;
- $f^{2k-2} \leq f^{2k-1}$, $f^{2k-2}(m) = f^{2k-1}(m)$ for $m > 2k - 1$;
- $f^{2k-1}(2k - 1) = \{ x \}$ for some $x$ of degree $p_k$.

To see this is possible, note that, as above, we assume without loss of generality that $\phi_n$ is defined within $F_{<p^{k+1}}$. Then we may apply theorem 2.2.1 for $K = F_{<p^k}$, $L = F_{<p^{k+1}}$ and $A = [L]^{<\omega}$, to show that there exists a set of polynomials $G \subset F_{<p}[X_1, \ldots, X_l]$ of degree at most $2^d(n)$ such that we can add $x$ in the manner described above if and only if $g(x, x, \ldots, x) \neq 0$ for all $g \in G$. But any $x \in F_{q^m}$ satisfies $[F_{<p^m}(x) : F_{<p^k}] = p_k > 2^d(n)$, but the degree of any $g \in G$ is at most $2^d(n)$, so $g(x, x, \ldots, x) \neq 0$, and such an approximation exists.
Bibliography
