On fields and groups

Jakub Gismatullin (Wrocław)

Model Theory Conference in celebration of Ludomir Newelski's 60th birthday

December 23, 2022

The talk is based on

1. join work with Katarzyna Tarasek[1] about some elementary aspects of algebraic closure of pseudofinite fields,
2. join work with Karol Kuczmarz[2] on metric groups and Gromov-Hausdorff distance,
3. join work with Krzysztof Majcher and Martin Ziegler[3] on metric ultraproducts.

[1] arXiv:2109.10130 J. Gismatullin & K. Tarasek, On binomials and algebraic closure of some pseudofinite fields, Communications in Algebra, 2023, VOL. 51, NO. 1, 95–97, DOI: 10.1080/00927872.2022.2088778

[2] `http://www.math.uni.wroc.pl/~gismat/gh.pdf`

[3] `arXiv:2010.03394`

A bit of memories: 2008, 2009

Figure: Barcelona 2008

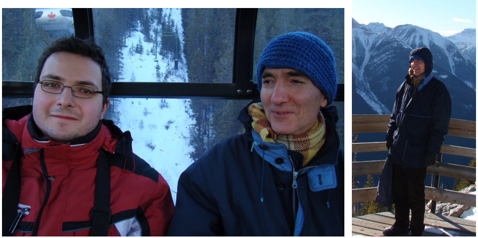

Figure: Banff (Canada) 2009

Year 2012

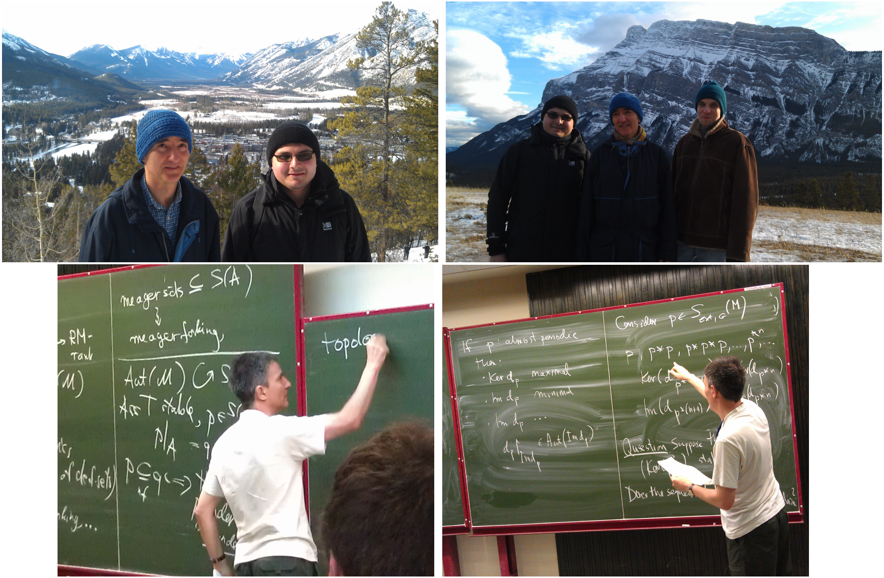

Figure: Banff & hard work in Wrocław

What is a binomial? When a binomial is irreducible?

A bit of reminder:

Definition

A *binomial* over a field K is a polynomial of the form $x^n - g$, where $n \in \mathbb{N}$ and $g \in K$.

Lemma

$x^n - g$ is irreducible over K if and only if [a]*:*

1. $g \notin K^p = \{x^p : x \in K\}$, *for each prime p, which divides n and*
2. *if $4|n$, then $g \notin -4K^4 = \{-4x^4 : x \in K\}$.*

[a] G. Karpilovsky, Topics in field theory, '89

Lemma

Let $\mathbb{F}_q$ be a finite field of cardinality $q = p^m$, p-prime. Then $x^n - g$, for $g \in \mathbb{F}_q$ is irreducible over $\mathbb{F}_q$ if and only if [a]*:*

1) $\mathrm{GCD}((q-1)/e, n) = 1$ *and every prime divisor of n divides e,*
2) *if $4|n$, then also $4|q-1$,*

where e is the order of g in the multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$.

[a] R. Lidl, H. Niederreiter. Finite fields, '97

Finite fields

$\mathbb{F}_q$ - finite field of cardinality $q = p^m$, p-prime
$\mathbb{F}_q^\times = \langle g_q \rangle$ is a cyclic group, generated by g_q

Lemma

$x^n - g_q$ is irreducible over $\mathbb{F}_q$ if and only if

$$\textit{every prime divisor of } n \textit{ divides } q-1 \textit{ and if } 4|n, \textit{ then } 4|q-1.$$

Example

For $q = 13$ take generator $g_{13} = 2$. Then

$x^n - 2$ is irreducible over $\mathbb{F}_{13} \Leftrightarrow$ each prime divisor of n must divide $q - 1 = 12 = 2^2 \cdot 3$, so n must be of the form $2^m \cdot 3^k$, $m, k \in \mathbb{N}$. Therefore each binomial

$$x^{2^m \cdot 3^k} - 2$$

is irreducible over $\mathbb{F}_{13}$.

Pseudofinite fields

A straightforward application of the Łoś ultraproduct theorem gives:

Theorem

Let $\mathbb{F}_{\bar{q}} = \prod_{k\in\mathbb{N}} \mathbb{F}_{q_k}/\mathcal{U}$ be an ultraproduct of $\{\mathbb{F}_{q_k}\}_{k\in\mathbb{N}}$ $\lim_{k\to\infty} q_k = \infty$ and let

$$g = ([g_k]_{k\in\mathbb{N}})_{\mathcal{U}} \in \mathbb{F}_{\bar{q}},\ \text{where each } g_k \text{ is a generator of } \mathbb{F}_{q_k}^{\times}.$$

Fix $n \in \mathbb{N}$ and let $\{\text{prime divisors of } n\} = \{p_1, \ldots, p_r\}$.
The following conditions are equivalent:

(1) $x^n - g$ *is irreducible over* $\mathbb{F}_{\bar{q}}$,

(2) *there exists* $h \in \mathbb{F}_{\bar{q}}$ *such that* $x^n - h$ *is irreducible over* $\mathbb{F}_{\bar{q}}$,

(3) *for* $\mathcal{U}$*-almost all* $k \in \mathbb{N}$:

$$p_1, p_2, \ldots, p_r \text{ divide } q_k - 1 \text{ and if } 4|n \text{ then } 4|q_k - 1.$$

A construction

Let us construct a pseudofinite field $\mathbb{F}_{\bar{q}}$ of characteristic zero and $g \in \mathbb{F}_{\bar{q}}$, such that

$$x^n - g \text{ is irreducible for every} n \in \mathbb{N}.$$

Example

$\{2 = p_1, p_2, \ldots\}$ - all prime numbers. Define a sequence $\{q_k : k \in \mathbb{N}\}$ of prime powers, such that

$$4, p_1, p_2, \ldots, p_k \text{ divide } q_k - 1 \text{ for all natural } k \in \mathbb{N}.$$

For example one can take

$$q_k = p_{k+1}^{(p_1-1)(p_2-1)\cdot\ldots\cdot(p_k-1)},$$

as then $p_i | q_k - 1 = {r_k}^{p_i - 1} - 1$ by the Fermat's little theorem. Take $\mathbb{F}_{\bar{q}} = \prod_{k\in\mathbb{N}} \mathbb{F}_{q_k}/\mathcal{U}$. Then by the Theorem: $x^n - g$ is irreducible over $\mathbb{F}_{\bar{q}}$, for all $n \in \mathbb{N}$.

Application

Application of Theorem and Example: handy description of algebraic closure of $\mathbb{F}_{\bar{q}}$

Theorem

If for some $g \in \mathbb{F}_{\bar{q}}$, for all $n \in \mathbb{N}$, $x^n - g$ is irreducible over $\mathbb{F}_{\bar{q}}$, then its algebraic closure $\widehat{\mathbb{F}_{\bar{q}}}$ is generated by $\left\{ \sqrt[n]{g} : n \in \mathbb{N} \right\}$ over $\mathbb{F}_{\bar{q}}$:

$$\widehat{\mathbb{F}_{\bar{q}}} = \mathbb{F}_{\bar{q}} \left(\sqrt[n]{g} : n \in \mathbb{N} \right) = \mathbb{F}_{\bar{q}} \left(g^{\mathbb{Q}} \right).$$

Compactness theorem implies:

Corollary

If $\mathbb{F}$ is a pseudofinite field which is ω-saturated and contains all roots of unity, then there is $g \in \mathbb{F}$ such that

$$\widehat{\mathbb{F}} = \mathbb{F} \left(g^{\mathbb{Q}} \right).$$

Metric group: bi-invariant norm and invariant metric on a group

Suppose G is a group.

$d\colon G \times G \to \mathbb{R}_{\geq 0}$ is an *invariant metric* on G, if

$$d(gx, gy) = d(x, y) = d(xg, yg)$$

for all $g, x, y \in G$

Each such invariant metric comes from a *bi-invariant (i.e. conjugacy invariant) norm (lenght)* $\|\cdot\|\colon G \to \mathbb{R}_{\geq 0}$ (another notation $\ell\colon G \to \mathbb{R}_{\geq 0}$) satisfying

- $\|gh\| \leq \|g\| + \|h\|$
- $\left\|g^{-1}\right\| = \|g\| = \|hgh^{-1}\|$
- $\|g\| = 0$ if and only if $g = e$ (pseudonorm, when only $\|e\| = 0$)

$$\|\cdot\| \quad \rightsquigarrow \quad d(x, y) = \left\|xy^{-1}\right\|$$

$$d(\cdot, \cdot) \quad \rightsquigarrow \quad \|g\| = d(g, e)$$

Examples of norms and lengths

Examples of bounded and unbounded norms

- Discrete norm: $\|g\| := \begin{cases} 1 & : g \neq e \\ 0 & : g = e \end{cases}$
- Hamming norm S_n: $\sigma \in S_n$, $\|\sigma\|_H := \|\{i \in \{1, \ldots, n\} : \sigma(i) \neq i\}\|$
- Rank norm on $\mathrm{GL}_n(F)$ (F: field) $\|g\|_r := rank(g - I)\,(= \dim(Im(g - I)))$
- Conjugacy length (pseudonorm) on a finite group G:

$$\ell_c(g) := \frac{\log |g^G|}{\log |G|}$$

it is a norm when $Z(G) = \{e\}$

Motivating question

How close to each other are two metric groups?

Let $(G_m, \|\cdot\|_m)_{m\in\mathbb{N}}$ be a family of metric groups.
Metric ultraproduct $\prod_{m\in\mathbb{N}}^{\text{met}} G_m$ is $G_{\text{fin}}/N_{\mathcal{U}}$ where

$$G_{\text{fin}} = \left\{ (g_m) \in \prod_{m\in\mathbb{N}} G_m : \sup_{m\in\mathbb{N}} \|g_m\|_m < \infty \right\} \text{ oraz } N_{\mathcal{U}} = \left\{ (g_m) : \lim_{m\to\mathcal{U}} \|g_m\|_m = 0 \right\}$$

Consider metric ultraproducts:

1. $\mathcal{S}_1 = \prod_{m\in\mathbb{N}}^{\text{met}} (S_\infty, \frac{1}{m}\|\cdot\|_H)$,
2. $\mathcal{S}_2 = \prod_{m\in\mathbb{N}}^{\text{met}} (S_\infty, \frac{1}{m^2}\|\cdot\|_H)$,

where $S_\infty = \bigcup_{n\in\mathbb{N}} S_n$. Both $\mathcal{S}_1$ and $\mathcal{S}_2$ are simple metric groups[4].

Question

What is $d_{GH}(\mathcal{S}_1, \mathcal{S}_2) =$?

[4] arXiv:2010.03394, JG, KM, MZ

Hausdorff and Gromov-Hausdorff distances

The Hausdorff distance $d_H(A, B)$ measures the distance of two sets A, B in a given metric space (X, d), and is defined as:

$$d_H(A, B) = \max \left\{ \sup_{a \in A} d(a, B),\ \sup_{b \in B} d(b, A) \right\}.$$

The Gromov-Hausdorff distance $d_{GH}(X, Y)$ goes a step further and tries to give the distance of two metric spaces X and Y. $d_{GH}(X, Y) = 0$ iff X and Y are isometric.

Gromov-Hausdorff distance $d_{GH}(X, Y)$ of two metric spaces (X, d^X) i (Y, d^Y) is defined via d_H between isometric embeddings of X and Y into an arbitrary metric space (Z, d^Z):

$$d_{GH}(X, Y) = \inf \left\{ d_H\Big(\phi_X[X], \phi_Y[Y]\Big) : \phi_X : X \to Z,\ \phi_Y : Y \to Z \text{ are isometries} \right\}.$$

This definition is very abstract. Let us use another equivalent definition.

Gromov-Hausdorff distance via distortion of correspondence

1. A *correspondence* $R \subseteq X \times Y$ between two sets X i Y is a subset of $X \times Y$ with full projections on X and Y: $\pi_1(R) = X$ and $\pi_2(R) = Y$
2. $\mathcal{R}(X, Y) =$ the family of *all* correspondences between X i Y
3. A *distortion* $\mathrm{dis}(R)$ *of* $R \in \mathcal{R}(X, Y)$ is:

$$\mathrm{dis}(R) = \sup_{(x,y),(x',y')\in R} \left| d^X(x,x') - d^Y(y,y') \right| .$$

The Gromov-Hausdorff distance $d_{GH}(X, Y)$ can be determined via distortions[5]:

$$d_{GH}(X, Y) = \frac{1}{2} \inf \{\mathrm{dis}(R) : R \in \mathcal{R}(X, Y)\} .$$

Example

Let $G = (\mathbb{Z}, d_{\mathbb{Z}})$, where $d_{\mathbb{Z}}(n, m) = |n - m|$. Consider $H = 2\mathbb{Z} < G$. Then

$$d_H(\mathbb{Z}, 2\mathbb{Z}) = 1 \text{ and } d_{GH}(\mathbb{Z}, 2\mathbb{Z}) = \frac{1}{2}.$$

Consider a correspondence $\mathfrak{R} \in \mathcal{R}(\mathbb{Z}, 2\mathbb{Z})$:

$$\mathfrak{R} = \{(2n, 2n), (2n + 1, 2n) : n \in \mathbb{Z}\}.$$

Then $\mathrm{dis}\,\mathfrak{R} = 1$, so $d_{GH}(\mathbb{Z}, 2\mathbb{Z}) = \frac{1}{2}$.

[5] D. Burago, Y. Burago, S. Ivanov. A course in metric geometry, '01

Hausdorff distance between permutation groups

Lemma

(G, d) - metric group, d- bi-invariant and $H < G$. Then

$$d_H(G, H) = \sup\{d(g, H) : g \in G\} = \sup\{d(g_i, H) : i \in I\},$$

where $\{g_i : i \in I\}$ is a set of representatives of all left cosets H in G.

Corollary

The Hausdorff distance between S_n and S_m with the Hamming metric is

$$d_H(S_n, S_m) = \begin{cases} 2(n-m) & : m \geq \frac{1}{2}n \\ n & : m < \frac{1}{2}n \end{cases}.$$

Hausdorff distance between some linear groups

Definition

Let $\mathbb{F}$ be a field, fix $n \in \mathbb{N}$, $n \geq 2$ and define:

$$\begin{aligned}
\mathrm{GL}_n(\mathbb{F}) &= \{M \in M_{n\times n}(\mathbb{F}) : \det(M) \neq 0\},\\
\mathrm{SL}_n(\mathbb{F}) &= \{M \in \mathrm{GL}_n(\mathbb{F}) : \det(M) = 1\},\\
\mathrm{T}_n(\mathbb{F}) &= \{M \in \mathrm{GL}_n(\mathbb{F}) : M \text{ is upper triangular}\},\\
\mathrm{UT}_n(\mathbb{F}) &= \{M \in \mathrm{T}_n(\mathbb{F}) : M \text{ has 1 on the diagonal}\},\\
\mathrm{Diag}_n(\mathbb{F}) &= \{M \in \mathrm{T}_n(\mathbb{F}) : M \text{ is diagonal matrix}\},\\
\mathrm{Sc}_n(\mathbb{F}) &= \{M \in \mathrm{Diag}_n(\mathbb{F}) : M = \lambda \cdot I \text{ for some } \lambda \in \mathbb{F} \setminus \{0\}\}.
\end{aligned}$$

Theorem

Let $n \geq m \geq 2 \in \mathbb{N}$. Then

$$\begin{aligned}
d_H(\mathrm{UT}_n(\mathbb{F}), \mathrm{UT}_m(\mathbb{F})) = d_H(\mathrm{T}_n(\mathbb{F}), \mathrm{T}_m(\mathbb{F})) &= n - m,\\
d_H(\mathrm{Diag}_n(\mathbb{F}), \mathrm{Diag}_m(\mathbb{F})) &= n - m, \ \textit{if } \mathbb{F} \neq \mathbb{F}_2,\\
d_H(\mathrm{T}_n(\mathbb{F}), \mathrm{UT}_n(\mathbb{F})) &= n, \ \textit{if } \mathbb{F} \neq \mathbb{F}_2,\\
d_H(\mathrm{T}_n(\mathbb{F}), \mathrm{T}_n(\mathbb{F}) \cap \mathrm{SL}_n(\mathbb{F})) &= 1, \ \textit{if } \mathbb{F} \neq \mathbb{F}_2.
\end{aligned}$$

Hausdorff distance - conjecture

Conjecture below is suggested by doing computations in GAP for small finite fields.

Conjecture

Let $\mathbb{F}$ be a field and $n, k \in \mathbb{N}_{>1}$. For $n > k$ consider $\mathrm{SL}_k(\mathbb{F})$ as diagonally embedded into $\mathrm{SL}_n(\mathbb{F})$. Then the following hold for any $n \in \mathbb{N}_{>1}$

1. $d_H(\mathrm{SL}_{n+1}(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})) = d_H(\mathrm{GL}_{n+1}(\mathbb{F}), \mathrm{GL}_n(\mathbb{F})) = 2,$
2. $d_H(\mathrm{SL}_{n+2}(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})) = d_H(\mathrm{GL}_{n+2}(\mathbb{F}), \mathrm{GL}_n(\mathbb{F})) = 4,$
3. $d_H(\mathrm{SL}_{n+3}(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})) = d_H(\mathrm{GL}_{n+3}(\mathbb{F}), \mathrm{GL}_n(\mathbb{F})) = 5.$

We could not compute $d_H(\mathrm{SL}_6(\mathbb{F}_2), \mathrm{SL}_2(\mathbb{F}_2))$ (computationally intractable problem), so we have no reasonable conjecture about this quantity.

Gromov-Hausdorff distance for permutation groups

General known results on Gromov-Hausdorff distance give us the following bounds:

$$\frac{1}{2}(n-m) \leq d_{GH}(S_n, S_m) \leq \frac{1}{2}n \text{ for } 1 < m < n.$$

We proved that:

Theorem

For $1 < m < n$:

1. $d_{GH}(S_n, S_m) \leq \frac{3}{2}(n-m)$, *for* $n \leq \frac{3}{2}m$,
2. $d_{GH}(S_n, S_m) = \frac{1}{2}n$, *for* $n > m!$,
3. $d_{GH}(S_n, S_m) \leq \frac{1}{2}(n-1)$, *for* $n \leq m!$, $n \geq 4$, $m \geq 3$,
4. $d_{GH}(S_n, S_m) \leq \frac{1}{2}(n-2)$, *for* $n \leq \frac{1}{2}\left(1+\sqrt{4m!+1}\right)$, $n \geq 5$, $m \geq 4$,
5. $d_{GH}(S_n, S_{n-1}) = {}^{3}\!/_{2}$, *for all* $n \geq 3$.

The exact value of $d_{GH}(S_n, S_m)$ is unknown, in the general case.

Gromov-Hausdorff distance for linear groups

Theorem

Suppose $\mathbb{F} \neq \mathbb{F}_2$. *Then*

$$d_H(\mathrm{GL}_n(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})) = 1, \quad d_{GH}(\mathrm{GL}_n(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})) = \frac{1}{2}.$$

Theorem

Let $G := \mathrm{GL}_n(\mathbb{F})$, $H := \mathrm{SL}_n(\mathbb{F})$ *and* $\mathbb{F} \neq \mathbb{F}_2$.

1. *Let* U *be a group such that* $H < U < G$. *Then we have that:*

$$d_H(G, U) = d_H(U, H) = 1, \quad d_{GH}(G, U) = d_{GH}(U, H) = \frac{1}{2}.$$

2. *Let* U *be a group such that* $\mathrm{Diag}_n(\mathbb{F}) < U < G$. *Then we have that:*

$$d_H(U, U \cap \mathrm{SL}_n(\mathbb{F})) = 1, \quad d_{GH}(U, U \cap \mathrm{SL}_n(\mathbb{F})) = \frac{1}{2}.$$

Gromov-Hausdorff distance - more conjectures

Conjecture below is suggested by doing intensive computational experiments.

Conjecture

1. $d_{GH}(\mathrm{GL}_n(\mathbb{F}), \mathrm{T}_n(\mathbb{F})) = d_{GH}(\mathrm{GL}_n(\mathbb{F}), \mathrm{UT}_n(\mathbb{F})) = \frac{n}{2}$
2. *If* $\mathbb{F} \neq \mathbb{F}_2$, *then* $d_{GH}(\mathrm{T}_n(\mathbb{F}), \mathrm{UT}_n(\mathbb{F})) = \frac{n}{2}$.
3. $d_{GH}(\mathrm{T}_n(\mathbb{F}), \mathrm{Diag}_n(\mathbb{F})) = \frac{n-1}{2}$

Thank you!