

Subsets of fields and arithmetic operations

S. Mattarei

Trento, Italy

Topics in Algebra
in honour of Professor A. E. Zaleskii
on the occasion of his 70th birthday
Milan, 13-15 May 2009

Let F be a field and let S be a subset of F .

- If S is closed with respect to subtraction and division then S is a subfield.
- How redundant are these conditions?
What if S is only “partially” closed with respect to these or other operations?
Can we still conclude that S is a subfield?
Is S at least close to a subfield in some way?

- 1 Nonsingular derivations of Lie algebras
- 2 Binomial coefficients modulo a prime
- 3 Addition and inversion

1 Nonsingular derivations of Lie algebras

2 Binomial coefficients modulo a prime

3 Addition and inversion

Derivations, and addition in a field

- Let D be a derivation of a Lie algebra.
If $Dv = \alpha v$ and $Dw = \beta w$ then

$$D[v, w] = [Dv, w] + [v, Dw] = (\alpha + \beta)[v, w].$$

If $[v, w] \neq 0$, it is an eigenvector for D . Same for generalized eigenvectors (in weight spaces).

- Reasonable expectation: if L is far from abelian then many Lie brackets will be nonzero, and hence many sums of eigenvalues of D will be eigenvalues. Then the spectrum of D will enjoy some degree of closure with respect to addition.

- A derivation is *nonsingular* if it is injective; equivalently, if 0 is not an eigenvalue.
- (Jacobson 1955) Let L be a finite-dimensional Lie algebra over a field of characteristic zero. If L admits a nonsingular derivation then L is nilpotent.
- This does not extend to positive characteristic: for each $k > 1$ there is a finite-dimensional simple Lie algebra of characteristic p , which has a semisimple derivation D with spectrum $\mathbb{F}_{p^k}^*$.
- Note that $D^{p^k-1} = 1$ here. In fact, D has exact order $p^k - 1$.

- A Lie algebra with a derivation D such that $D^{p-1} = 1$ cannot be simple. In fact, it must be nilpotent. This plays a role in Shalev's effective proof of the coclass conjectures for finite p -groups.



A. Shalev

The structure of finite p -groups: effective proof of the coclass conjectures

Invent. Math. **115** (1994), 315–345

Problem (Shalev)

Describe \mathcal{N}_p , the set of positive integers n which occur as the orders of nonsingular derivations of non-nilpotent Lie algebras of characteristic p .



A. Shalev

The orders of nonsingular derivations

J. Austral. Math. Soc. Ser. A **67** (1999), 254-260

- If n is in \mathcal{N}_p then all multiples of n are.
- If n is in \mathcal{N}_p then its p' -part is.
- $p^k - 1 \in \mathcal{N}_p$ for any $k > 1$.
These and their multiples are *the trivial elements* of \mathcal{N}_p .

Theorem (Shalev (\Rightarrow)/Mattarei (\Leftarrow))

*n prime to p belongs to \mathcal{N}_p if, and only if,
there exists $\alpha \in \bar{\mathbb{F}}_p$ with $(\alpha + \lambda)^n = 1$ for all $\lambda \in \mathbb{F}_p$.*

- Equivalently, the subgroup of $\bar{\mathbb{F}}_p^*$ of order n contains a “line” $\alpha, \alpha + 1, \dots, \alpha + p - 1$.
- Using this characterization one finds that $(p^k - 1)/(p - 1) \in \mathcal{N}_p$, for all $k \geq 1$.
Hence \mathcal{N}_p has nontrivial elements when p is odd.
- $73 = (2^9 - 1)/7$ is a nontrivial element of \mathcal{N}_2 .



S. Mattarei

The orders of nonsingular derivations
of modular Lie algebras

Israel J. Math. **132** (2002), 265-275

- (Shalev) No number in \mathcal{N}_p is less than $p^2 - 1$.
- (Mattarei) The numbers in \mathcal{N}_p less than $p^3 - 1$, for $p > 3$, are multiples of $p^2 - 1$.

Open question

Is it true that, given r , for all sufficiently large primes p all numbers $n \in \mathcal{N}_p$ which are *less than* $p^r - 1$ are multiples of some $p^k - 1$?

- (Mattarei) Given r , for all sufficiently large primes p all numbers $n \in \mathcal{N}_p$ which *divide* $p^r - 1$ are multiples of some $p^k - 1$.

Large divisors of $p^k - 1$ belong to \mathcal{N}_p

Theorem

*If n divides $q - 1 = p^k - 1$ and $n^p \geq (p - 1)q^{p - \frac{1}{2}}$,
then $n \in \mathcal{N}_p$.*

- A simpler sufficient condition is $n \geq 1.32 \cdot q^{1 - \frac{1}{2p}}$.
- If $(p^k - 1)/d$ is an integer then it belongs to \mathcal{N}_p provided $k \geq 2 + 2p \log d / \log p$.
- For example, $(3^k - 1)/2 \in \mathcal{N}_3$ for $k \geq 6$ (and also for $k = 3, 4, 5$, as one verifies).
For k prime these are nontrivial elements of \mathcal{N}_3 .



S. Mattarei

The orders of nonsingular derivations
of Lie algebras of characteristic two
Israel J. Math. **160** (2007), 23-40



S. Mattarei

A sufficient condition for a number to be the order of a
nonsingular derivation of a Lie algebra
Israel J. Math. (2009), in press

1 Nonsingular derivations of Lie algebras

2 Binomial coefficients modulo a prime

3 Addition and inversion

- Consider a finite field \mathbb{F}_q , and a subgroup G of \mathbb{F}_q^* .
- If $G \cup \{0\}$ is closed under subtraction then $G \cup \{0\}$ is a subfield.
- G being a subgroup, the hypothesis is equivalent to:
 $1 - \alpha \in G$ for all $\alpha \in G \setminus \{1\}$.
- How much can we weaken this hypothesis while keeping the same conclusion?

A sample question

Suppose that H is a proper subgroup of G
and that $1 - \alpha \in G$ for all $\alpha \in G \setminus H$.

Does it follow that $G \cup \{0\}$ is a subfield of \mathbb{F}_q ?

For $|G| = k$ and $|H| = h$ the hypothesis means:
 $(1 - x^k)/(1 - x^h)$ divides $(1 - x)^k - 1$.

Hence

$$\begin{aligned} \sum_{i=1}^k (-1)^i \binom{k}{i} x^i &= (1 - x)^k - 1 \\ &= g(x) \cdot (1 - x^k)/(1 - x^h) \\ &= g(x) \cdot \sum_{j=0}^{k/h-1} x^{jh} \end{aligned}$$

for some $g(x) \in x\mathbb{F}_p[x]$, of degree h .

Therefore,

$$(-1)^{i+h} \binom{k}{i+h} \equiv (-1)^i \binom{k}{i} \pmod{p}$$

for $0 \leq i \leq k - h$.

Note that $h \mid k$ by Lagrange's theorem, hence $h \leq k/2$.

Periodicity of binomial coefficients

- Now suppose that $(-1)^i \binom{k}{i} \pmod{p}$ is periodic as a function of i , in the range $0 \leq i \leq k$, with period length h .
Need not assume that $h \mid k$.

- One case is when $k + 1$ is a power of p :

$$\binom{p^f - 1}{i} \equiv (-1)^i \pmod{p} \quad \text{for } 0 < i < k.$$

- It turns out this is the only case of periodicity, provided the period h is not too long with respect to k .
 $h \leq k/2$ is enough but, more precisely...

Theorem

Let p be a prime, $k \geq 5$, $p \nmid h$ and $0 < 3h < 2k + 5$. If

$$\binom{k}{i+h} \equiv (-1)^h \binom{k}{i} \pmod{p}$$

for $0 \leq i \leq k - h$, then $k + 1$ is a power of p .

- Similar results holds for unsigned binomial coefficients, and/or periodicity with respect to the “numerator” k .



S. Mattarei

Modular periodicity of binomial coefficients

J. Number Theory **117** (2006), 471-481

A question with a weaker hypothesis

Suppose that $1 - \alpha \in G$ for at least half the elements α of G .
In a formula, $|G \cap (1 - G)| \geq |G|/2$.
Does it still follow that $G \cup \{0\}$ is a subfield of \mathbb{F}_q ?

- If $|G| = k$ and $n = (q - 1)/k$, then $G = \{\beta^n : \beta \in \mathbb{F}_q^\times\}$.
- We have an n^2 -to-one correspondence between

$$\{(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : x^n + y^n = 1\}$$

and $G \cap (1 - G)$, given by $(\beta, \gamma) \mapsto \beta^n$.

- Hence $|G \cap (1 - G)| = (N - d)/n^2$,
where N is the number of projective \mathbb{F}_q -rational points of the Fermat curve $x^n + y^n = z^n$,
and d is the number of those with $xyz = 0$, namely,
 $d = 3n$ if $|G|$ is even and $d = 2n$ otherwise.
- Weil's bound $|N - q - 1| \leq (n - 1)(n - 2)\sqrt{q}$ holds,
but is not enough here:
it only implies that either $G = \mathbb{F}_q^*$ or $|G| < 2\sqrt{q}$.
- The problem is that Weil's bound is only efficient
when n is small with respect to q .

- A periodicity relation is a special case of a linear recurrence relation.
- A sequence $(s_i)_{i \geq 0}$ satisfies a linear recurrence relation of degree h if

$$s_i = a_1 s_{i-1} + a_2 s_{i-2} + \cdots + a_h s_{i-h}$$

for $i \geq h$, where a_i are suitable constants with $a_h \neq 0$.

- The definition can be adjusted to deal with finite sequences.

No linear recurrence for binomial coefficients

Subsets of
fields and
arithmetic
operations

Mattarei

Nonsingular
derivations of
Lie algebras

Binomial
coefficients
modulo a
prime

Addition and
inversion

Theorem

Let p be a prime and h, k integers with $0 \leq 2h \leq k < p - h$. Then the finite sequence $\binom{k}{i} \pmod{p}$, for $i = 0, \dots, k$, does not satisfy any linear recurrence relation of degree h .

- It extends to characteristic zero by reading $p = \infty$.
- The assumption $2h \leq k$ is sharp, and natural: when $2h > k$ a linear recurrence relation always exists.



S. Mattarei

Linear recurrence relations for binomial coefficients
modulo a prime

J. Number Theory **128** (2008), 49-58

- Suppose that G is a subgroup of \mathbb{F}_q^* and that $G \cup \{0\}$ is not a subfield. We asked earlier whether $|G \cap (1 - G)| < |G|/2$.
- When $k = |G| < p - 1$ a positive answer follows from the above theorem:

Corollary

Let G be a subgroup of \mathbb{F}_q^ with $|G| < p - 1$.*

Let $a, b \in \mathbb{F}_q^$, and set $e = 0, 1, 2, 3$ according as none, one, two or all three of a, b and $-a/b$ (counting repetitions) belong to G . Then $|aG \cap (1 - bG)| \leq (|G| + 1 - e)/2$.*

Other bounds for Fermat curves

- This gives a new proof of a known bound for the number of \mathbb{F}_p -rational points of the curve $ax^n + by^n = 1$.
- That bound is the first of a sequence of bounds for $|G \cap (1 - G)|$, each linear in $|G|$ (Garcia and Voloch, 1988).
Taken together, they give

$$|G \cap (1 - G)| \leq c \cdot |G|^{2/3}$$

for some (small) constant c .

- 1 Nonsingular derivations of Lie algebras
- 2 Binomial coefficients modulo a prime
- 3 Addition and inversion**

Problem

Describe all additive subgroups S of a field E such that $S \setminus \{0\}$ is closed with respect to taking inverses.

Apart from subfields there is one natural example:

Example

$\text{char}(E) \neq 2, \quad K \subset L \subseteq E, \quad |L : K| = 2, \quad S = \ker \text{Tr}_{L/K}.$

In fact, if ψ is the nonidentity automorphism of L/K , then

$$s \in S \iff \psi(s) = -s,$$

and for $s \neq 0$ that is equivalent to $\psi(s^{-1}) = -s^{-1}$.

Hua's identity (1949)

In any associative ring we have

$$a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba,$$

as long as a, b and $ab - 1$ are invertible.

Consequently, an inverse-closed additive subgroup S of E is invariant under the binary operation $(a, b) \mapsto aba = a^2b$. Using this one easily finds all possibilities for S .

Inverse-closed additive subgroups

Theorem

*If E is a field of characteristic not two
and $S \neq \{0\}$ is an inverse-closed additive subgroup,*

- *either S is a subfield,*
- *or S is the set of elements of trace zero
in a quadratic field extension contained in E .*

Theorem

*If E is a field of characteristic two
and $S \neq \{0\}$ is an inverse-closed additive subgroup,
then S is an F^2 -subspace of F , for some subfield F of E .*

The special case of finite fields

The case of finite fields is of special interest because of cryptographic applications of the inversion map (question raised by A. Caranti).

Alternate proof for finite fields.

If E has $q = p^f$ elements, then $f(x) = \prod_{s \in S} (x - s)$ is a monic divisor of $x^q - x$. Now

S is addition-closed $\iff f$ is a p -polynomial,

and

$S \setminus \{0\}$ is inverse-closed $\iff f(x)/x$ is self-reciprocal.

Both conditions together hold exactly when f is a binomial of the form $x^{p^r} \pm x$, for some divisor r of f . \square



S. Mattarei

Inverse-closed additive subgroups of fields

Israel J. Math. **159** (2007), 343–348

- The following paper includes the same results, but also deals with the harder case of division rings (of characteristic not two), which relies on Jordan theory.



D. Goldstein, R. Guralnick, L. Small, E. Zelmanov

Inversion invariant additive subgroups of division rings.

Pacific J. Math. **227** (2006), 287–294.