Overview of C_i-fields and motivation

Def. (Lang) Let $i \in \mathbb{Z}_{\geq 0}$. A field k is called a C_i-field if every homogeneous polynomial in k of degree $d \geq 1$ satisfying $n > d^i$ has a non-trivial zero. ($n = \#$ variables)

Lemma. $k = \bar{k} \iff k$ is C_0

($C_i \Rightarrow C_{i+1}$)

Examples

- $\mathbb{F}_3$ is not C_0. Take $F = x^2 + y^2$, $(x,y) \neq (0,0)$ then $F(x,y) \neq 0$
- $\mathbb{F}_2$ " $F = x^2 + xy + y^2$
- $\mathbb{R}$ is not C_i for any i. $F = X_1^{2d} + \dots + X_n^{2d}$ if $n > (2d)^i$

Thm. If k is a finite field, then k is C_1.

$$17XY^2 + 4Z^3 + 3WZ^2 + W^3$$

Thm (Lang, Tsen/Lang-Nagata, Greenberg)

Let k be a C_i-field, then:

- any algebraic extension of k is C_i
- $k(t)$ is C_{i+1}-field
- $k((t))$ is C_{i+1}-field

Thm (Ax-Kochen) "$\mathbb{Q}_p$ is almost C_2".

Thm (Chevalley-Warning)
Let $f \in \mathbb{F}_q[x_1, \dots, x_n]$, with char $\mathbb{F}_q = p > 0$ and $d = \deg(f)$.

Write $N(f) = \#$ distinct zeros of f in $\mathbb{F}_q$.

If $n > d$, then $N(f) \equiv 0 \mod p$

Lemma $\displaystyle\sum_{x \in \mathbb{F}_q^*} x^m = \begin{cases} -1 & \text{if } q-1 \mid m \\ 0 & \text{otherwise} \end{cases}$ if $m \geq 1$

Proof. • If $q-1 \mid m \Rightarrow x^{q-1} = 1 \quad \forall x \in \mathbb{F}_q^*$
$\Rightarrow x^m = 1 \quad \forall x \in \mathbb{F}_q^*$

So $\displaystyle\sum_{x \in \mathbb{F}_q^*} x^m = q-1 = -1$

• If $q-1 \nmid m$, $\exists y \in \mathbb{F}_q^*$ s.t. $y^m \neq 1$.

$$\sum_{x \in \mathbb{F}_q^*} x^m = \sum_{x \in \mathbb{F}_q^*} (yx)^m = y^m \sum_{x \in \mathbb{F}_q^*} x^m \Rightarrow \sum_{x \in \mathbb{F}_q^*} x^m = 0$$

$\square$

Proof. For $\underline{x} \in \mathbb{F}_q^n$ we have $1 - f(\underline{x})^{q-1} = \begin{cases} 1 & \text{if } \underline{x} \text{ is a zero} \\ 0 & \text{otherwise} \end{cases}$

$$\overline{N(f)} = \overline{\sum_{\underline{x} \in \mathbb{F}_q^n} \left(1 - f(\underline{x})^{q-1}\right)} = -\sum_{\underline{x} \in \mathbb{F}_q^n} f(\underline{x})^{q-1}$$

$= \mathbb{F}_q$- linear combination of monomials of degree $\leq d(q-1)$

Let $x_1^{\mu_1} \dots x_n^{\mu_n}$ be such a monomial, then

$$\sum_{\underline{x} \in \mathbb{F}_q^n} x_1^{\mu_1} \dots x_n^{\mu_n} = \prod_{i=1}^{n} \boxed{\left(\sum_{x_i \in \mathbb{F}_q} x_i^{\mu_i} \right)}$$

If all μ_i would satisfy $\mu_i \geq q-1$, then

$$d(q-1) \geq \deg(x_1^{\mu_1} \dots x_n^{\mu_n}) = \sum \mu_i \geq n(q-1) > d(q-1)$$

So for some i we have $0 \leq \mu_i < q-1$

Hence $N(f) \equiv 0 \mod p$.

Relation of C_1 to Brauer groups

Def • A central simple algebra (CSA) over K is a fin. dimensional associative algebra over K, whose two sided ideals are precisely $\{0\}$ and itself and whose center is K.

• A central division algebra (CDA) over K is a CSA/K s.t. all non-zero elements are invertible.

Example

• K and $M_n(K)$ are CSA/K

• $\mathbb{H} = \{ \mathbb{R}1 + \mathbb{R}\underline{i} + \mathbb{R}\underline{j} + \mathbb{R}\underline{k} \mid \underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -1,\ \underline{ij} = \underline{k}, \underline{jk} = \underline{i}, \underline{ki} = \underline{j}.$

$$(a + b\underline{i} + c\underline{j} + d\underline{k})(a - b\underline{i} - c\underline{j} - d\underline{k}) = a^2 + b^2 + c^2 + d^2$$

So $\mathbb{H}$ is a CDA/$\mathbb{R}$

Properties of CSA's

A be a CSA/K

• $\exists$ a finite Galois extension L/K s.t. $L \otimes_K A \cong M_n(L)$

$A \hookrightarrow L \otimes_K A$, so we may assume $A \subset M_n(L)$.
$a \longmapsto 1 \otimes a$

$$\dim_K A = \dim_L M_n(L) = n^2.$$

• If A, B are CSA's/K, then so is $A \otimes_K B$

$(a \otimes b) \cdot (c \otimes d) = ac \otimes bd$

• A^{opp} "opposite algebra", same underlying vector space as A, but multiplication is defined by $a * b = \underbrace{ba}_{\text{product in } A}$

We have $\underline{A \otimes_K A^{opp} \cong M_n(K)}$, where $n^2 = \dim_K A$.

$\underline{K \otimes_K A \cong A}$.

Example

$\longrightarrow$ $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong M_2(\mathbb{C})$ $\quad a + b\underline{i} + c\underline{j} + d\underline{k} \longmapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$

Thm (Wedderburn)

If A is a CSA$/K$, then $A \cong M_n(D)$ for some unique $n \geq 1$ and a unique central division algebra D.

$\longrightarrow$ If A, B are CSA's$/K$, define $A \sim B \iff M_r(A) \cong M_s(B)$ for some $r, s > 0$.

For instance $K \sim M_n(K)$

$\mathbb{R} \not\sim \mathbb{H}$ since $\underset{\text{no zero divisors}}{\mathbb{H}} \not\cong \underset{\text{lots of zero divisors}}{M_2(\mathbb{R})}$ $\quad M_r(\mathbb{H}) \not\cong M_s(\mathbb{R})$

$\mathbb{H} \cong M_n(D)$ so $n = 1$, $D = \mathbb{H}$

Brauer Group$/K$: $\quad Br(K) = \{ [A] \mid A \text{ is CSA}/K \}$

with $[A] \cdot [B] := [A \otimes_K B]$

$[A] \cdot [A^{opp}] = [M_n(K)] = \underline{[K]}$

$[K] \cdot [A] = [K \otimes A] = [A]$.

Examples:
- $Br(\bar{k}) = \{ [\bar{k}] \}$ $\quad \left(\bar{k} \otimes_{\bar{k}} A \cong M_n(\bar{k}) \right)$ $\quad [\bar{k}] \cdot [A] = [\bar{k}]$
- $Br(\mathbb{R}) = \{ [\mathbb{R}], [\mathbb{H}] \} \cong \mathbb{Z}/2\mathbb{Z}$
- $Br(\mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z}$

Thm

If K is a C_1-field, then $Br(K) = \{[K]\}$.

$\Rightarrow$ $Br(\mathbb{F}_q)$ is trivial.

{Proof. Assuming the only central division algebras over K are K itself.}

Let A be CSA$/K$, by Weddernburn: $A \cong M_n(D) = M_n(K)$
$[A] = [M_n(K)] = [K]$.

Let D be a central division algebra $/K$, $\exists$ finite Galois extension L/K s.t. $L \otimes D \cong M_n(L)$, so $\dim_K D = n^2$ and wlog assume $D \subseteq M_n(L)$.

Fix a K-basis $\{\omega_1, \ldots, \omega_{n^2}\}$ of D $(\omega_i \in M_n(L))$, we define

$$Nred(\underline{x}) = \det(x_1\omega_1 + \cdots + x_{n^2}\omega_{n^2}) \quad (x_i \text{ are intermediates})$$
$$\in L[x_1, \ldots, x_{n^2}]$$

$Nred(\lambda \underline{x}) = \lambda^n \, Nred(\underline{x})$, so $Nred(\underline{x})$ is homogeneous of degree n.

Let $\sigma \in Gal(L/K)$, then σ is a K-automorphism of $M_n(L)$.
So by Skolem-Noether $\exists B \in GL_n(L)$ s.t.
$$\sigma(A) = BAB^{-1} \quad \forall A \in M_n(L). \leftarrow$$

$$\begin{aligned}\sigma(Nred(\underline{x})) &= \det(x_1\sigma(\omega_1) + \cdots + x_{n^2}\sigma(\omega_{n^2})) \\ &= \det(x_1 B\omega_1 B^{-1} + \cdots + x_{n^2} B\omega_{n^2} B^{-1}) \\ &= Nred(\underline{x})\end{aligned}$$

$\Rightarrow$ $Nred(\underline{x})$ is actually an element of $K[x_1, \ldots, x_{n^2}]$

For $x, y \in D$ we have $N_{red}(x) N_{red}(y) = N_{red}(xy)$

D is a division algebra : for $x \neq 0$, we have

$N_{red}(x) \, N_{red}(x^{-1}) = 1$

So over K the only zero of $N_{red}(\underline{x})$ is $(0, \ldots, 0)$.

Since K is C_1 we cannot have that $n^2 > d = n$.

So we must have that $n^2 \leq n \Rightarrow n = 1$

Meaning that K is the only CDA over itself

$\square$

For $0 \leq i < 1$ we have $C_i = C_0$

Open: Does $\exists \; i \geq 1, \; i \notin \mathbb{Z}$ s.t. K is C_i but not $C_{\lfloor i \rfloor}$
and K