Lecture 1: Philosophy and basic notions

Thursday, January 19, 2017 9:21 AM

Fields come up a lot.

Natural

- Algebraic Geometry: fields of functions on varieties
  "Birational geometry"
- Number theory: finitely generated fields
  touches on deep problems – Tate conjecture
- Analysis: fields of meromorphic functions on $\mathbb{C}$-analytic manifolds

Unnatural: limits ((very) infinite) of field extensions

- making fields bigger often makes them (structurally) simpler

<u>Questions</u>

- notions of closeness / size?
  (valuations / completions)
- notion of dimension?
  (transcendence degrees, p-basis, cohomological dim, Diophantine dim, Brauer dim, ...)
- positivity / orders? how many?

(real orderings, Harrison topology)

- What Galois gps are there, and how do they fit together?
  (Inverse Gal problem)

- How to construct Gal exts "explicitly"?
  (Generic Galois theory)

- How can we interpret fields as functions on a variety or similar object?
  (Grothendieck's Anabelian Conjectures)

Approach

Basic strategy for exploring field arithmetic: translate questions in terms of poly eqns.

Given a system of eqns, when can you solve it?

More rationally, due to limited brain size, we restrict to certain special systems

simple to writedown

simple to interpret

$f(\vec{x})=0$

f deg d hom.

$x \in A$ is a zero divisor

$(x_1, --, x_\ell)$ spans a ℓ-dim'l

$f(\bar{x})=0$

f deg d hom.

Tsen-Lang thy

"Diophantine dim"

$(x_1,\dots,x_l)$ spans a l-dim'l right ideal of A.

↕

Algebraic structures over fields.

Fundamental tool - glue together various perspectives

Galois Cohomology

analog of singular cohom of a top space.

↙ invariants of field

↘ measuring devices for structures over field

Milnor conjecture (Voevodsky)

Bloch-Kato conjecture / Norm residue isom thm (Voevodsky, Weibel, ---)

Actual Math

Def A Monoid $M=(M,\cdot,1)$ is a set w/ operation $\cdot$ which is associative, $\underset{m\cdot 1}{\underset{\shortparallel}{1\cdot m}}=m$ all m

Def A monoid is *cancellative* if $mn = m'n \Rightarrow m = m'$
and $nm = nm' \Rightarrow m = m'$

Def A group is a monoid where every elmt is invertible.

Def An (associative unital) ring is ...

0-ring is a ring.

Def A commutative domain is a ring R s.t. $(R \setminus \{0\}, \cdot)$ is a cancellative monoid

Def A commutative domain R is a field if $(R \setminus \{0\}, \cdot)$ is a gp.

Def A *prime field* is a field w/ no proper subfields

Prop $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $\mathbb{Q}$ are the only prime fields and every field contains a unique prime field.

Pf: consider
$$\begin{aligned} \mathbb{Z} &\to F \\ 1 &\mapsto 1 \end{aligned}$$

$1 \longmapsto 1$

Def Charactristic. = min'l non-negative generatr of kernel

Field Extensions

Def if $F \subset E$ field extension

(also write E/F)

we say E is a simple extension of F if

$\exists\, \alpha \in E$ s.t. $E = F(\alpha)$

Note: in the case that $F(\alpha)/F$ is a finite ext.

$1, \alpha, \alpha^2, \ldots, \alpha^n$ lin. dependent for some min'l n,

then α satisfies some poly f of min'l degree

over F, and we have

$$F(\alpha) \xleftarrow{\sim} F[x]/f(x)$$

$$\alpha \longleftarrow\!\shortmid\; x$$

& $f(x)$ irreducible

More generally, hom's from simple exts

$$\begin{tikzcd} \frac{F[x]}{f(x)} = F(\alpha) \arrow[r] & L \\ & F \arrow[ul] \arrow[u] \end{tikzcd}$$

correspond to

sending α to any

root of $f(x)$

Def E/F is a splitting field for a poly $f(x)$ if $E = F(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n \in E$ and are all the roots of $f(x)$.

Def $f(x) \in F[x]$ is seperable if it has distinct roots in a splitting field.

Def E/F separable if whenever $f(x)$ is irred poly which factors in E w/ lin factors, then $f(x)$ is separable.

Def E/F normal if whenever $f(x)$ irred w/ root in E, then E contains a splitting field for $f(x)$

Thm Dedekind Lemma

Suppose G is a group, F a field, $\chi_1, \dots, \chi_n$ are pairwise distinct group homomorphisms

$$\chi_i : G \longrightarrow F^*$$

Then, thought of as elements of the vector space $Map(G,F)$, these are independent.

Pf: Suppose $\sum_i a_i \chi_i(x) = 0$ all $x \in G$.

induction n

By hypothesis, we know $\chi_1(g) \neq \chi_2(g)$ some $g \in G$

substitute gx for x $\rightsquigarrow$ $\sum_i a_i \chi_i(gx) = 0$

$$\sum_i a_i \chi_i(g) \chi_i(x) = 0$$

subtract

mult. by $\chi_1(g)$

$$\sum_i a_i \chi_1(g) \chi_i(x) = 0 \qquad \sum_i a_i \left(\chi_i(g) - \chi_1(g)\right) \chi_i(x) = 0$$

$$\Downarrow$$

$$0 = \sum_{i=2}^{n} a_i \left(\chi_i(g) - \chi_1(g)\right) \chi_i(x)$$

$$\Rightarrow a_i \left(\chi_i(g) - \chi_1(g)\right) = 0 \quad \text{all } i$$

$$a_2 (\underbrace{\chi_2(g) - \chi_1(g)}_{\neq 0}) = 0$$

$$\Rightarrow a_2 = 0$$

$\sum_{i \neq 2} a_i \chi_i(x) = 0$ all x $\Rightarrow$ done by induction. $\square$

Consequently, if we let $\sigma_1, \dots, \sigma_m$ be aut's of a field extension E/F, then we can apply this by setting $G = E^*$ $\quad E^* \xrightarrow{\sigma_i} E^*$

by setting $G = E^*$ $\qquad E^* \xrightarrow{\sigma_i} E$

$\Longrightarrow \sigma_1, \ldots, \sigma_m$ independent in $\mathrm{Hom}_F(E,E)$

$$\begin{tikzcd}\mathrm{Hom}_F(E,E) \arrow[d, phantom, "\cap"] \\ \mathrm{Maps}(E^*,E)\end{tikzcd}$$

be careful : vector space in 2 different ways.

$\sigma \in \mathrm{Aut}(E) \subset \mathrm{Hom}_F(E,E)$, $x \in E$

(mult. of thm) $x \cdot \sigma \in \mathrm{Hom}_F(E,E)$ (left mult)

$$x \cdot \sigma = \quad y \longmapsto x\sigma(y)$$

alternate mult. $\sigma \cdot x \in \mathrm{Hom}_F(E,E)$ (right mult)

$$\sigma \cdot x = \quad y \longmapsto \sigma(xy) = \sigma(x)\sigma(y)$$

Note: if $\dim_F E = [E:F] = n$ then

$\dim_F \mathrm{Hom}_F(E,E) = n^2$

Since $\sigma_1, \ldots, \sigma_m$ distinct auts of $E/F \Longrightarrow$

$$\underbrace{\bigoplus_{i=1}^{m} E\sigma_i}_{mn \text{ dim'l}} \subset \underbrace{\mathrm{Hom}_F(E,E)}_{n^2 \text{ dim'l}} \Longrightarrow m \leq n$$

Def/Thm : a finite field ext. E/F is Galois if the following equivalent properties are true

1. E/F is normal & separabl
2. $|\mathrm{Aut}_F(E)| = [E:F]$
3. $\bigoplus_{\sigma \in \mathrm{Aut}_F(E)} E\sigma \longrightarrow \mathrm{End}_F(E)$ is an isomorphism

$= (E, G, 1)^{\alpha/}$

Consider the algebra structure on left

<u>Def</u> If F a field, an F-algebra A is an $\overset{F}{\text{vector}}$ space w/ ringstructure s.t. if $\lambda \in F$, $x, y \in A$ then

$$\lambda(xy) = (\lambda x)y = x(\lambda y)$$

$$(\text{i.e. } \lambda \in Z(A) = \{ z \in A \mid zx = xz \text{ all } x \in A \}$$

$$(x\sigma)(y\tau)(z) = (x\sigma)\, y\tau(z) = x\,\sigma(y)\,\sigma\tau(z)$$

$z \in E$

$$\quad\quad\quad\quad\quad\quad\quad\quad \overset{\shortparallel}{(x\,\sigma(y))\,\sigma\tau\ (z)}$$

$$\Rightarrow (x\sigma)(y\tau) = x\,\sigma(y)\,\sigma\tau$$

$$(E, G, 1)$$