ALGEBRA II 2024

eero.hakavuori@helsinki.fi C316

TA: jonathan.pim@helsinki.fi

Lectures: Tuesday & Thursday 14.15-16.00 B322

Exercises: Wednesday 14.15-16.00 B322

- problems published previous Thursday
- Solutions checked in person on Wednesday

Evaluation: 2 exams (18 pts + 18 pts) + exercises (6 pts)

- exams based on material in lectures + exercises
- exercises 1 pt for each 15% completed

Reference material

- Stewart, Galois theory 5.ed
- Cox, Little, O'shea, Ideals varieties and algorithms 4.ed
- Handwritten notes

COURSE OUTLINE

- Field extensions
- Multivariate polynomial rings and Gröbner bases
- Algebra - geometry dictionary
  (Ideal - variety correspondence)

<u>Definition 0</u> (Polynomial ring $K[x_1, \dots, x_n]$)

- A <u>monomial</u> in the indeterminates $x_1, \dots, x_n$ is a product $\underbrace{x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}}$, $\alpha_i \in \mathbb{N}$.
  Multi-index notation: $=: x^\alpha$, $\alpha = (\alpha_1, \dots, \alpha_n)$
- The <u>polynomial ring</u> $K[x_1, \dots, x_n]$ over a field K in the indeterminates $x_1, \dots, x_n$ is the set of all K-linear combinations of monomials:

$$p = \sum_{\alpha \in A} a_\alpha x^\alpha \quad , \quad A \text{ Finite set of multi-indices } \alpha$$

1. FIELD EXTENSIONS

Concretely, we will consider

subring of $\mathbb{C}$: $R \subset \mathbb{C}$ s.t. $1 \in R$ and
$x, y \in R \Rightarrow x+y, -x, xy \in R$

subfield of $\mathbb{C}$: subring $K \subset \mathbb{C}$ s.t. $0 \neq x \in K \Rightarrow x^{-1} \in K$

Abstractly,

Field of characteristic 0 : $1+1+1+1+\ldots \neq 0$

Definition 1.1

Let K, L be fields.

A field extension is a monomorphism $K \hookrightarrow L$

[we will routinely identify K as a subset of L]

Warning: Standard notation L/K "L over K"

will be avoided in this course to avoid confusion with quotients

Example 1.2

Let $K = \mathbb{Q}$ and consider the polynomial

$$f(t) = t^4 - 4t - 5 = (t^2+1)(t^2-5) \in \mathbb{Q}[t]$$

irreducible in $\mathbb{Q}[t]$

In the field extension $\mathbb{Q} \hookrightarrow \mathbb{C}$ can factor completely

$$f(t) = (t-i)(t+i)(t-\sqrt{5})(t+\sqrt{5})$$

[But $\mathbb{C}$ contains many irrelevant elements, e.g. π, $\sqrt[3]{7}$, ...]

Definition 1.3

Let $X \subset \mathbb{C}$ be a subset.

- The <u>subfield of $\mathbb{C}$ generated by X</u> is the unique smallest subfield containing X
- The field extension $K \hookrightarrow L$ is <u>generated over K by X</u> if L is generated by $K \cup X$. Denoted $L = K(X)$
- If X is finite, $L = K(X)$ is a <u>finitely generated extension</u>
- If X is a singleton $X = \{\alpha\}$, $L = K(X) = K(\alpha)$ is a <u>simple extension</u>

Example 1.4

Let $X = \{i, \sqrt{5}\}$, $L = \mathbb{Q}(i, \sqrt{5})$

Claim: $L = \{a + bi + c\sqrt{5} + di\sqrt{5} : a,b,c,d \in \mathbb{Q}\}$

Proof: sums and products straightforward

For inverses, direct computation is messy.

Consider instead $\mathbb{Q} \hookrightarrow \underbrace{\mathbb{Q}(i)}_{=:\tilde{L}} \hookrightarrow \mathbb{Q}(i, \sqrt{5}) = \tilde{L}(\sqrt{5})$

and show $\tilde{L} = \{a + bi : a,b \in \mathbb{Q}\}$

Inverses contained in $\tilde{L}$: $(a+bi)^{-1} = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2} i$

Then $a + bi + c\sqrt{5} + di\sqrt{5} = z + w\sqrt{5}$, $z, w \in \tilde{L}$

and $(z + w\sqrt{5})(z - w\sqrt{5}) = z^2 - 5w^2 \in \tilde{L}$ has an inverse in $\tilde{L}$

$\Rightarrow (z + w\sqrt{5})^{-1} = (z - w\sqrt{5})(z^2 - 5w^2)^{-1} \in \tilde{L}(\sqrt{5})$

[Note: why is $z^2 - 5w^2 \neq 0$? Hint: real vs imaginary, rational vs irrational]

Example 1.5 Let K be a field

The field of rational functions over K

in the indeterminates $x_1, \dots, x_n$

$$K(x_1,\dots,x_n) = \left\{ \frac{p(x_1,\dots,x_n)}{q(x_1,\dots,x_n)} : p,q \in K[x_1,\dots,x_n] \right\}$$

is a field extension of K:

the monomorphism $K \hookrightarrow K(x_1,\dots,x_n)$ is the map onto constants.

[Note similarity in notation to field generated by X]

Lemma 1.6

Let $X \subset \mathbb{C}$ be nonempty and $X \neq \{0\}$, and $K \subset \mathbb{C}$ subfield.

Then $K(X)$ is the subset of all elements of $\mathbb{C}$

obtained by a finite sequence of field operations

using elements of K and X.

Proof

Let F be the set of elements obtained from field operations.

$F \subset K(X)$ follows since $K(X)$ is a field and $K \cup X \subset K(X)$

By definition $K(X)$ is the smallest subfield containg $K \cup X$.

$\Rightarrow$ suffices to show F is a field, since $K \cup X \subset F$.

If $x, y \in F$ obtained by finite sequence, then $xy, x+y, x^{-1}$ also finite.

$\square$

Definition 1.7

An <u>isomorphism of field extensions</u> $K \hookrightarrow L$ and $\hat{K} \hookrightarrow \hat{L}$ is a pair (λ, μ) of field isomorphisms such that we obtain a commutative diagram

$$\begin{tikzcd} L \arrow[r, "\lambda"] & \hat{L} \\ K \arrow[u, hook] \arrow[r, "\mu"] & K \arrow[u, hook] \end{tikzcd}$$

Example 1.8.

$\mathbb{Q} \hookrightarrow \mathbb{Q}(i, \sqrt{5})$ and $\mathbb{Q} \hookrightarrow \mathbb{Q}(i+\sqrt{5})$ are isomorphic

Example 1.4 $\Rightarrow$ $\mathbb{Q}(i, \sqrt{5}) = \{a + bi + c\sqrt{5} + di\sqrt{5} : a,b,c,d \in \mathbb{Q}\}$

Goal :

$$\begin{tikzcd} \mathbb{Q}(i+\sqrt{5}) \arrow[r, "\lambda"] & \mathbb{Q}(i, \sqrt{5}) \\ \mathbb{Q} \arrow[u, hook] \arrow[r, "\mu"] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

Set $\mu = \mathrm{id}$.

Claim: the inclusion $\lambda : \mathbb{Q}(i+\sqrt{5}) \hookrightarrow \mathbb{Q}(i, \sqrt{5})$ is a field isomorphism.

Injectivity and homomorphism immediate. Check surjectivity:

$$(i+\sqrt{5})^0 = 1 \rightsquigarrow (1, 0, 0, 0)$$
$$(i+\sqrt{5})^1 = i + \sqrt{5} \rightsquigarrow (0, 1, 1, 0)$$
$$(i+\sqrt{5})^2 = 4 + 2i\sqrt{5} \rightsquigarrow (4, 0, 0, 2)$$
$$(i+\sqrt{5})^3 = 14i + 2\sqrt{5} \rightsquigarrow (0, 14, 2, 0)$$

image has 4 $\mathbb{Q}$-linearly independent vectors $\Rightarrow$ surjective.

Proposition 1.9

Let $\tau: K \hookrightarrow L$ be a field extension.

Then L is a vector space over K, (K = scalars)

where scalar multiplication is defined through τ by

$$k \cdot a := \underbrace{\tau(k) \cdot a}_{\text{multiplication in } L} \qquad k \in K,\ a \in L$$

Proof

Each property of a vector space follows immediately from the field structure on L (exercise) $\square$

Definition 1.10

- The degree of a field extension $K \hookrightarrow L$ is
  $$[L:K] = \dim_K(L) \qquad \text{(dimension as } K\text{-vector space)}$$
- an extension is finite if $[L:K] < \infty$.

Example 1.11

i) Examples 1.4 & 1.7 $\Rightarrow$ $[\mathbb{Q}(i,\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(i+\sqrt{5}):\mathbb{Q}] = 4$

ii) $[\mathbb{C}:\mathbb{R}] = 2$ since $\{1, i\}$ is a $\mathbb{R}$-basis of $\mathbb{C}$.

Theorem 1.12 (Tower law; multiplicativity of degree)

If $K \hookrightarrow L \hookrightarrow M$ field extensions, then

$$[M:K] = [M:L]\cdot[L:K]$$

(also makes sense when one or both extensions infinite)

Corollary 1.13

If $K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n$ field extensions, then

$$[K_n:K_0] = [K_n:K_{n-1}]\cdot\ldots\cdot[K_1:K_0]$$

Proof of Thm 1.12

Let $\{x_i : i\in I\}$ be a K-basis of L

$\{y_j : j\in J\}$ be a L-basis of M

Claim: $\{x_i y_j : (i,j)\in I\times J\}$ is a K-basis of M.

If so, then the thm follows since

$$\dim_K M = |I\times J| = |I|\cdot|J| = \dim_K L\cdot \dim_L M$$

Proof of claim:

i) linear independence of $x_i y_j$:

If $\sum_{i,j} k_{ij}x_i y_j = 0$, $k_{ij}\in K$ then $\sum_j\left(\sum_i k_{ij}x_i\right)y_j = 0$.

L-Linear independence of $\{y_j\}$ $\Rightarrow$ $\sum_i k_{ij}x_i = 0\in L$ $\forall j\in J$.

K-linear independence of $\{x_i\}$ $\Rightarrow$ $k_{ij}=0$ $\forall i\in I$ $\forall j\in J$

ii) $x_i y_j$ span all of M:

Let $m\in M$. $\{y_j\}$ L-basis $\Rightarrow$ $m = \sum_j l_j y_j$, $l_j\in L$.

$\{x_i\}$ K-basis $\Rightarrow$ each $l_j = \sum_i k_{ij}x_i$ $\Rightarrow m = \sum_{i,j} k_{ij}x_i y_j$ $\square$