4.8 Normal bases

<u>Def:</u> L/K finite Galois of degree n

$Gal(L/K) = \{\sigma_1, \dots, \sigma_n\}$

A <u>normal basis for L/K</u> is a basis of the form

$(\sigma_1(a), \dots, \sigma_n(a))$ for some $a \in L$.

<u>Thm 1:</u> Every finite Galois extension has a normal basis.

<u>proof:</u> $\to$ Here only for infinite fields; the case of finite fields is treated later.

- K infinite
  L/K finite Galois
  $Gal(L/K) = \{\sigma_1 = id_L, \sigma_2, \dots, \sigma_n\}$
  By Thm. 3.2.10, L/K has a primitive element a, i.e. $L = K(a)$. Let f be the minimal polynomial of a over $K \Rightarrow f = \prod_{i=1}^{n}(T - a_i)$ for $a_i = \sigma_i(a)$. (in $L[T]$)

- Define

$$g_i = \frac{f}{(T-a_i)\cdot f'(a_i)} = \frac{1}{\prod_{j \neq i}(a_i - a_j)} \cdot \prod_{j\neq i}(T - a_j),$$

which are in $L[T]$ $(i = 1, \dots, n)$. Then

$$g_i(a_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

$\Rightarrow$ $g_1 + \dots + g_n - 1 \in L[T]$ has n different roots $a_1, \dots, a_n$

Since $\deg g_i = \deg f - 1 = n-1$, this implies that $g_1 + \dots + g_n = 1$.

- Since $(T-a_k)$ divides $g_i g_j$ for all k and $i \neq j$, we have
$$g_i g_j \equiv 0 \pmod{f} \quad (\text{for } i \neq j)$$

Thus
$$g_i = g_i \cdot (g_1 + \dots + g_n) = g_i g_1 + \dots + g_i g_n$$
$$\equiv g_i^2 \pmod{f}$$

- Define $D = (\sigma_k \sigma_i (g_1))_{i,k=1\dots n} \in \mathrm{Mat}_{n \times n}(L[T])$

Since $a_i = \sigma_i(a)$ and $\sigma_1 = \mathrm{id}_L$, we have
$$a = a_1 \quad \text{and} \quad \sigma_i(g_1) = g_i.$$

Thus
$$D \cdot D^T \equiv \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \pmod{f}$$

$\Rightarrow (\det D) \cdot (\det D^T) \equiv 1 \pmod{f}$

$\Rightarrow \det D \in L[T]$ is not trivial

$\Rightarrow (\det D)(s) \neq 0$ for some $s \in L$ (since L is infinite), i.e. if $c = g_1(s)$, then $\det(\sigma_k \sigma_i(c))_{i,k=1\dots n} \neq 0$.

- Consider

$$\lambda_1 \sigma_1(c) + \dots + \lambda_n \sigma_n(c) = 0$$

with $\lambda_1 \dots \lambda_n \in K$. Applying $\sigma_1 \dots \sigma_n$ yields

$$\begin{aligned} \lambda_1 \sigma_1 \sigma_1(c) + \dots + \lambda_n \sigma_1 \sigma_n(c) &= 0 \\ \vdots \qquad\qquad & \quad \vdots \\ \lambda_1 \sigma_n \sigma_1(c) + \dots + \lambda_n \sigma_n \sigma_n(c) &= 0 \end{aligned}$$

Since $\det(\sigma_k \sigma_i(c))_{i,k} \neq 0$, this implies that $\lambda_1 = \dots = \lambda_n = 0$. Thus $\sigma_1(c), \dots, \sigma_n(c)$ are linearly independent over K and $(\sigma_1(c), \dots, \sigma_n(c))$ forms a normal basis for L/K. $\square$

<u>Lemma 2:</u> L/K finite Galois

$G = Gal(L/K)$

$(\sigma(a))_{\sigma \in G}$ normal basis for L/K for $a \in L$

(1) $H < G$

Then

$$L^H = \left\{ \sum_{\sigma \in G} c_\sigma \sigma(a) \;\middle|\; \begin{array}{l} c_\sigma \in K \text{ s.t. } c_\sigma = c_{\tau\sigma} \\ \text{for all } \sigma \in G, \tau \in H \end{array} \right\}$$

(2) $H \triangleleft G$

$I \subset G$ set of representatives for G/H

$b = \sum_{\tau \in H} \tau(a)$

Then $(\sigma(b))_{\sigma \in I}$ is a normal basis

for L^H/K.

proof: (1) Consider $\sum_{\sigma \in G} c_\sigma \cdot \sigma(a) \in L$. For $\tau \in H$, we have

$$\tau\Big(\sum_{\sigma \in G} c_\sigma \cdot \sigma(a)\Big) = \sum_{\tau\sigma \in G} c_\sigma \, \tau\sigma(a) = \sum c_{\tau^{-1}\sigma}\, \sigma(a).$$
$$\left(\begin{smallmatrix} \tau\sigma \mapsto \tau^{-1}\tau\sigma = \sigma \\ \sigma \mapsto \tau^{-1}\sigma \end{smallmatrix}\right)$$

Thus $\tau\big(\sum c_\sigma \sigma(a)\big) = \sum c_\sigma \sigma(a) \quad (\forall \tau \in H)$

$\iff c_\sigma = c_{\tau^{-1}\sigma}$ for all σ $(\forall \tau \in H)$.

(2) For $\sigma \in G$, we have $\sigma H = H\sigma$.

$\Rightarrow \sigma(b) = \sum_{\tau \in H} \sigma\tau(a) = \sum_{\tau \in H} \tau\sigma(a) = \sum_{\tau \in H} \tau(\sigma(a))$

is invariant under H, i.e. $\sigma(b) \in L^H$.

By (1), $(\sigma(b))_{\sigma \in I}$ spans L^H over K.

Since $\# G/H = [L^H : K]$, it is a basis for L^H/K. Since

$(\sigma(b))_{\sigma \in I} = (\sigma(b))_{\sigma \in \underbrace{Gal(L^H/K)}_{\simeq G/H}}$, it

is a normal basis. $\square$

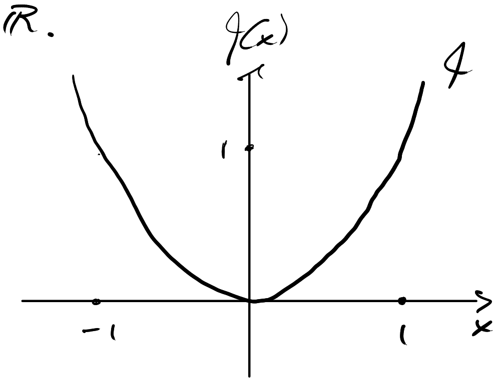
4.9 The fundamental theorem of algebra

<u>Thm 1:</u> $\mathbb{C}$ is algebraically closed.

<u>proof:</u> We need from analysis:

<u>Fact 1:</u> $a \in \mathbb{R}$

Then $a \geq 0$ iff $a = b^2$ for some $b \in \mathbb{R}$.



<u>proof:</u> "$\Leftarrow$": $f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ has image in $\mathbb{R}_{\geq 0}$.

"$\Rightarrow$": For every $a \geq 0$ $\exists\, c >> 0$ s.t. $f(0) = 0 \leq a \leq c^2 = f(c)$.

By the intermediate value theorem, there is a $b \in [0, c]$ s.t. $f(b) = a$. ∎

<u>Fact 2:</u> $f \in \mathbb{R}[T]$ of odd degree and monic

Then f has a root $a \in \mathbb{R}$.

<u>proof:</u> $f(b) < 0$ for $b << 0$

$f(c) > 0$ for $c >> 0$

$\Rightarrow$ By the intermediate value theorem,

$f(a) = 0$ for some $a \in [b, c]$. ∎

<u>claim 1:</u> Every $z \in \mathbb{C}$ has a square root.

<u>proof:</u> Write $z = a + bi$ with $a, b \in \mathbb{R}$. By Fact 1, there are $c, d \in \mathbb{R}$ s.t.

$$c^2 = \frac{1}{2}\underbrace{\left(a + \sqrt{a^2 + b^2}\right)}_{\geq 0} \quad \text{and} \quad d^2 = \frac{1}{2}\underbrace{\left(-a + \sqrt{a^2 + b^2}\right)}_{\geq 0}.$$

$$\Rightarrow (c + di)^2 = c^2 - d^2 + 2cdi = a + bi.$$ ∎

Let $L/\mathbb{C}$ be a finite field extension. After enlarging L, we can assume that $L/\mathbb{R}$ is Galois (and thus $L/\mathbb{C}$).

$$\begin{tikzcd} L \arrow[d, dash, "\text{Galois}"] \arrow[dd, dash, bend right, "\text{Galois}"'] \\ \mathbb{C} \arrow[d, dash] \\ \mathbb{R} \end{tikzcd}$$

<u>Claim 2:</u> $L = \mathbb{C}$.

Let $G = \mathrm{Gal}(L/\mathbb{R})$, $H < G$ a 2-Sylow subgroup and $E = L^H$. Then $E/\mathbb{R}$ is of odd degree $\#(G/H)$. By Thm. 3.2.10, $E = \mathbb{R}(a)$ for some primitive element $a \in E$. Let f be the minimal polynomial of a over $\mathbb{R}$, which is monic of odd degree.

$$\begin{tikzcd} & L \arrow[dl, dash, "2^a"'] \arrow[dr, dash] & \\ E \arrow[dr, dash, "\text{odd}"'] & & \mathbb{C} \arrow[dl, dash, "2"] \\ & \mathbb{R} & \end{tikzcd}$$

By Fact 2, f has a root in $\mathbb{R}$, which is only possible if $f = T - a$. Thus $E = \mathbb{R}$, and $G = H$ is a 2-group.

- Thus also $G' = \mathrm{Gal}(L/\mathbb{C}) < G$ is a 2-group. Either $G' = \{e\}$ ($\Rightarrow L = \mathbb{C}$ as claimed) or G' has a composition series

$$\{e\} = H_0 \underset{\mathbb{Z}/2}{\triangleleft} \text{—} \underset{\mathbb{Z}/2}{\triangleleft} H_{r-1} \underset{\mathbb{Z}/2}{\triangleleft} H_r = G'$$

$$\begin{tikzcd} L \arrow[d, dash] \\ F = L^{H_{r-1}} \arrow[d, dash] \\ \mathbb{C} = L^H \end{tikzcd}$$

with $r \geq 1$ by Lemma 4.2.5. Thus $F = L^{H_{r-1}}/\mathbb{C}$ has Galois group $\mathbb{Z}/2\mathbb{Z}$. Since $\zeta_2 = -1 \in \mathbb{C}$, $F/\mathbb{C}$ is Kummer and thus $F = \mathbb{C}(a)$

for a root $a \in F$ of a polynomial

$f = T^2 - b \in \mathbb{C}[T]$ (Thm. 4.5.1).

But by claim 1, $a = \sqrt{b} \in \mathbb{C}$. $\lightning$

Since $L = \mathbb{C}$ for every finite $L/\mathbb{C}$,

$\mathbb{C} = \{ a \in \overline{\mathbb{C}} \mid a \text{ algebraic over } \mathbb{C} \}$

is algebraically closed. $\square$