H13 Algebraïsch Afgesloten lichamen

def Een lichaam heet algebraïsch afgesloten als voor elke $f \in K[X]$, $f \notin K$, er een $\alpha \in K$ is met $f(\alpha) = 0$

— in feite splijt elke $f \in K[X] - K$ volledig in lineaire factoren

St 13.2 Zij K algebraïsch afgesloten. Dan is equivalent

1. elk irred. polynoom $f \in K[X]$ is lineair
2. de enige algebraïsche uitbreiding L van K is $L = K$
3. voor elke monische $f \in K[X]$ zijn er $\alpha_1, \dots, \alpha_n \in K$ met $f = \prod_{i=1}^{n} (X - \alpha_i)$

Bew. algebr. afgesl $\Rightarrow$ 1. : zij K algebr. afgesloten
een irreducibel polynoom f kan niet van graad ≥ 2 zijn want dan $f = (X - \alpha) q$ voor $\alpha \in K$ nulpunt, en q heeft graad ≥ 1 dus is niettriviaal en dus is f reducibel.
tevens kunnen elem. van $K \subset K[X]$ niet irred. zijn want als ze niet-0 zijn, zijn het eenheden

$1 \Rightarrow 2.$: Zij L algebraïsche uitbreiding van K
neem $\alpha \in K$. Dan is f_K^α monisch en irreducibel dus volgt wegens 1. dat het lineair is. Dat kan alleen als $f_K^\alpha = X - \alpha$, dus $\alpha \in K$. dus $L \subset K$ en omdat $K \subset L$ volgt $L = K$

$2 \Rightarrow 3.$ het ontbindingslichaam Ω_K^f is algebraïsch over K, want $\Omega_K^f = K(\alpha_1, \dots, \alpha_n)$ en eindige lich. over K zijn altijd algebraïsch over K als de geadjungeerde elementen $\alpha_1, \dots, \alpha_n$ algebraïsch zijn (10.4) $\Rightarrow \Omega_K^f = K$ want alle algebr. uitbr. van K zijn K zelf $\Rightarrow f$ splijt in K in $(X - \alpha_1) \cdots (X - \alpha_n)$

3. $\Rightarrow$ algebr. afg. welnu, $\alpha_i \in K$ en dit is een nulpunt van f dus $f \notin K$ heeft telkens een nulpunt α_i; $i = 1, \ldots n$ in K want $n \geq 1$ ($gr(f) = n$) $\square$

13.3 Elk algebraisch afgesloten lichaam is oneindig (equiv: er is geen $\mathbb{F}_q$ die algebr. afgesl. is)

Bew. Stel $K = \{e_1, e_2, \ldots e_n\}$ voor $n \in \mathbb{N}$. Dan bekijken we het polynoom

$$f = 1 + \prod_{i=1}^{n} (X - e_i) \quad \in K[X]$$

Dit is niet constant polynoom want $1 \neq 0$ en dus $n \geq 2$, dus $gr(f) \geq 2$. En $\forall e \in K$ $f(e) = 1 + 0 = 1 \neq 0$ dus dit is een polynoom zonder nulpunten in K tegenspraak met afgeslotenheid $\square$

De volgende stelling stond bekend als "H.S. v.d. Algebra"

St. 13.4 $\mathbb{C}$ is algebraisch afgesloten.

We geven geen direct bewijs maar eerst 4 lemma's waarin wat interessante weetjes over $\mathbb{C}$ naar boven zullen komen. Overigens kan H.S. Algb. niet puur algebraisch bewezen worden!

Lemma 13.5 (een niet-algebraisch argument) zij $f \in \mathbb{R}[X]$ en laat $\beta, \gamma \in \mathbb{R}$ met $f(\beta) > 0$ en $f(\gamma) < 0$. Dan is er een $\alpha \in \mathbb{R}$ met $f(\alpha) = 0$

Bewijs is natuurlijk dat $x \mapsto f(x) : \mathbb{R} \to \mathbb{R}$ een continue functie is dus uit (analyse) tussenwaardestelling volgt dat er een α tussen β en γ is met $f(\alpha) = 0$ omdat $\beta > 0 > \gamma$. $\square$

lemma 13.8 Zij $f \in \mathbb{C}[X]$ tweedegraads polynoom. Dan heeft f een nulpunt $\alpha \in \mathbb{C}$.

Bew neem zwa dat f monisch is: $f = X^2 + \beta X + \gamma$ met $\beta, \gamma \in \mathbb{C}$. Dan $f = (X + \frac{1}{2}\beta)^2 - (\frac{1}{4}\beta^2 - \gamma)$ volgt dat het voldoende is om te laten zien dat $\frac{1}{4}\beta^2 - \gamma \in \mathbb{C}$ een "wortel" $\alpha \in \mathbb{C}$ heeft met $\alpha^2 = \frac{1}{4}\beta^2 - \gamma$

Schrijf dus $\frac{1}{4}\beta^2 - \gamma = a + bi$ voor $a, b \in \mathbb{R}$.

$b=0$ Als $b=0$, dan moeten we aantonen dat er een $\alpha \in \mathbb{C}$ is met $\alpha^2 = a$. Maar we weten voor $g = X^2 - a \in \mathbb{R}[X]$ waarvoor $g(a+1) = a^2 + a + 1$, $g(a) = -a$, geldt als $a > 0$ dan $g(a+1) > 0$ $g(0) < 0$ dus met lemma 13.5 is er een $\alpha \overset{\in \mathbb{R} \subset \mathbb{C}}{\text{met}}$ $\alpha^2 - a = 0$ dus $\alpha^2 = a$. Als $a < 0$ dan passen we het toe op $|a| > 0$ en dan nemen we $\alpha = i\sqrt{|a|}$. Als $a = 0$ dan is $0^2 = 0$.

$b \neq 0$ we zoeken $c, d \in \mathbb{R}$ met $(c+di)^2 = a + bi$. dus desda: $c^2 + d^2 = a$, $2cd = b$

en $b \neq 0$ dus $c \neq 0$ en $d \neq 0$ dus we kunnen schrijven

$c = \frac{b}{2d} \Rightarrow \frac{b^2}{4d^2} - d^2 = a \Rightarrow d$ is reëel nulpunt van $g = 4X^4 - b^2 + 4aX^2$

en we zien dat $g(0) = -b^2 < 0$
en dat $g = 4(X^2 + a)X^2 - b^2$ dus voor $\beta > \frac{b}{2}$
en $\beta > \sqrt{|a|}$ volgt $g(\beta) > 0$.

Met 13.5 is er dus zo'n $d^{>0}$ en we vinden dan c uit $c = \frac{b}{2d}$ $\rightarrow$ dit bewijst existentie ih a.

$\square$

13.7 Zij $f \in \mathbb{R}[X]$ polynoom van oneven graad. Dan heeft f een nulpunt in $\mathbb{R}$

bew. neem zvva dat de kopcoeff > 0 is Dan $f(x) > 0$ als $x \in \mathbb{R}$ voldoende groot en $f(x) < 0$ als $x \in \mathbb{R}$ voldoende klein. Dus met 13.5 heeft f nulp. in $\mathbb{R}$ $\square$

13.8 Stel dat elke $f \in \mathbb{R}[X]$, $f \notin \mathbb{R}$ een nulpunt in $\mathbb{C}$ heeft. Dan is $\mathbb{C}$ algebraïsch afgesloten, dwz elke $f \in \mathbb{C}[X]$, $f \notin \mathbb{C}$ heeft een nulpunt in $\mathbb{C}$.

Bew neem $g = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$ TB g heeft nulpunt in $\mathbb{C}$

Zij $\bar{g} := \sum_{i=0}^{n} \bar{a}_i X^i$ waar $\bar{a}_i$ de complex geconjugeerde van a_i is.

Gaan we na dat $\bar{g} \cdot \bar{h} = \overline{gh}$ in $\mathbb{C}[X]$, gezien

$$\left(\sum_{i=0}^{n} \bar{a}_i X^i\right)\left(\sum_{i=0}^{m} \bar{b}_i X^i\right) = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} \bar{a}_i \bar{b}_i\right) X^i = \sum_{i=0}^{m+n}\left(\sum_{j+k=i} \overline{a_i b_i}\right) X^i$$

$$= \overline{\sum_{i=0}^{m+n}\left(\sum_{j+k=i} a_i b_i\right) X^i} = \overline{gh}$$, volgt:

zij $f = g \cdot \bar{g}$, dan $\bar{f} = \overline{g \cdot \bar{g}} = \bar{g} \cdot \bar{\bar{g}} = \bar{g} \cdot g = f$
dus $\forall i$ "$(f)_i \in \mathbb{R}$" $\Rightarrow f \in \mathbb{R}[X]$

bovendien $gr(f) = gr(g) + gr(\bar{g}) = 2\,gr(g) \geq 2$ dus f is geen constante. Heeft f een nulpunt in $\mathbb{C}$, dan $f = (X - \alpha)\, q$ voor een $q \in \mathbb{C}[X]$ en bovendien $g \cdot \bar{g} = (X - \alpha)\, q$ en $(X - \alpha)$ is irred. dus omdat $\mathbb{C}[X]$ een ontbring is (zelfs een hoofdideaaldomein) volgt $(X - \alpha) \mid g$ of $(X - \alpha) \mid \bar{g}$.

Of, in andere woorden, $0 = f(\alpha) = g(\alpha) = \bar{g}(\alpha)$
$\Rightarrow g(\alpha) = 0$ of $\bar{g}(\alpha) = 0$

Als $g(\alpha) = 0$ zijn we klaar.

Anders $\bar{g}(\alpha) = 0$ dus $\sum_{i=0}^{n} \bar{a}_i \alpha^i = 0 \Rightarrow \sum_{i=0}^{n} a_i \bar{\alpha}^i = 0$

Bewijs van H.S. Algebra volgt nu door:

— Zij $f \in \mathbb{R}[X]$ niet-constant. Volgens lemma 13.8 is het voldoende een nulp. van f in $\mathbb{C}$ aan te tonen.

— We mogen aannemen dat f monisch is. Zij $n = gr(f) \geq 1$ (want $f \notin \mathbb{R}$). Dan schrijven we $n = 2^k u$ met u oneven positief geheel en $k \geq 0$. We bewijzen met inductie naar $k \geq 0$ dat f een nulp. in $\mathbb{C}$ heeft.

— $k=0$: dan is $gr(f)$ oneven $\overset{13.7}{\Rightarrow}$ f heeft nulp. in $\mathbb{R} \subset \mathbb{C}$.

— $k \geq 1$: Stel we weten het al voor $k-1$. Laten we nu werken in de uitbreiding $L = \Omega_{\mathbb{C}}^{f} \supset \mathbb{C}$

In $L[X]$ splijt f volledig: $f = \prod_{i=1}^{n}(X-\alpha_i)$, $\alpha_i \in L$

Zij $c \in \mathbb{R}$ willekeurig en beschouw

$$g_c = \prod_{1 \leq i < j \leq n} \left(X - (\alpha_i + \alpha_j + c\alpha_i\alpha_j) \right) \qquad \in L[X]$$

Elk van de coëfficienten van g_c is een $\sigma_k \in \mathbb{R}[X_1, \dots, X_n]$ toegepast op $(\alpha + \alpha_j + c\alpha_i\alpha_j)_{1 \leq i < j \leq n}$
dwz $\sigma_k(\alpha_1 + \alpha_2 + c\alpha_1\alpha_2, \alpha_1 + \alpha_3 + c\alpha_1\alpha_3, \dots \alpha_{n-1} + \alpha_n + c\alpha_{n-1}\alpha_n)$
voor $k = 1, \dots, n$.
als we een α_i met $\alpha_j, i \neq j$ verwisselen, correspondeert dat met verwisselen van de termen $\alpha_\ell + \alpha_i + c\alpha_\ell\alpha_i$ met de termen $\alpha_\ell + \alpha_j + c\alpha_\ell\alpha_j$ voor $1 \leq \ell < \min\{i,j\}$
en verwisselen van de termen α

(want $\alpha_\ell + \alpha_j + c\alpha_\ell\alpha_j$ wordt $\alpha_\ell + \alpha_i + c\alpha_\ell\alpha_i$
en $\alpha_j + \alpha_\ell + c\alpha_j\alpha_\ell$ wordt α

maar onder het verwisselen van deze termen is σ_k invariant per symmetrie $\Rightarrow \sigma_k(\alpha_1 + \alpha_2 + c\alpha_1\alpha_2 \dots)$ zijn symm. in α_i:

Maar de symmetrische uitdrukkingen $\sigma_k(X_1+X_2-cX_1X_2,\dots)\in\mathbb{R}[X]$ hebben voor $\alpha_1,\dots\alpha_n\in\Omega_{\mathbb{C}}^{f}$ waarden in $\mathbb{R}$ omdat $\alpha_1,\dots\alpha_n$ nulp. van een polynoom $f\in\mathbb{R}[X]$ zijn. (Stelling 7.5)

$\Rightarrow g_c\in\mathbb{R}[X]$ $\forall c\in\mathbb{R}$. De graad van g_c is nu gelijk aan $\#\{(i,j)\in\mathbb{N}\times\mathbb{N} : 1\leq i<j\leq n\} = \frac{1}{2}n(n-1)$

$= \frac{1}{2}2^k u(n-1) = 2^{k-1}u(n-1)$ en $u(n-1)$ is even dus er zitten 2^{k-1} machten van 2 in $gr(g_c)\Rightarrow$ met (IH) volgt dus dat g_c een nulpunt in $\mathbb{C}$ heeft.

en de nulpunten van g_c zijn precies $\alpha_i+\alpha_j+c\alpha_i\alpha_j$ met $1\leq i<j\leq n$.

Dus voor elke $c\in\mathbb{R}$ zijn er i en j met $1\leq i<j\leq n$ en $\alpha_i+\alpha_j-c\alpha_i\alpha_j\in\mathbb{C}$

Er zijn oneindig veel reëele getallen en slechts eindig $(\frac{1}{2}n(n-1))$ veel (i,j), dus er zijn twee reële getallen $c\neq d\in\mathbb{R}$ met dezelfde i en j zodat dit geldt:

$\alpha_i+\alpha_j+c\alpha_i\alpha_j\in\mathbb{C}$ $\quad\alpha_i+\alpha_j+d\alpha_i\alpha_j\in\mathbb{C}$

nemen we geschikte $\mathbb{R}$-lineaire combinaties in $\mathbb{C}$, dan volgt $(c-d)\alpha_i\alpha_j\in\mathbb{C}$, $c\neq d$ dus

$\Rightarrow \gamma=\alpha_i\alpha_j = (c-d)^{-1}(c-d)\alpha_i\alpha_j\in\mathbb{C}$

en $c(\alpha_i+\alpha_j)+(c-d)\alpha_i\alpha_j-(d(\alpha_i+\alpha_j)+(d-c)\alpha_i\alpha_j)\in\mathbb{C}$

$\Rightarrow\dots\Rightarrow \underbrace{\alpha_i+\alpha_j}_{\beta}\in\mathbb{C}$

dus $(X-\alpha_i)(X-\alpha_j) = X^2-\beta X+\gamma\in\mathbb{C}[X]$

Lemma 13.6 geeft dat dit tweedegraads polynoom $\in\mathbb{C}[X]$ een nulp. in $\mathbb{C}$ heeft, dus $\alpha_i\in\mathbb{C}$ of $\alpha_j\in\mathbb{C}$ en dus heeft f een nulpunt in $\mathbb{C}$ QED

$\square$

— Gevolg van H.S. Algebra :

elk irred. polynoom $f \in \mathbb{R}[X]$ heeft graad 1 of 2
elke $X^2 + bX + c \in \mathbb{R}[X]$ is irred <u>desda</u>
$b^2 - 4c < 0$

bew. zij f monisch irred $\in \mathbb{R}[X]$ en $\alpha \in \mathbb{C}$
nulpunt van f. Dan $f = f^{\alpha}_{\mathbb{R}}$ en dan
vinden we $gr(f) = [\mathbb{R}(\alpha) : \mathbb{R}] \underset{)}{\leq} [\mathbb{C} : \mathbb{R}] = 2$
omdat $\mathbb{R}(\alpha) \subseteq \mathbb{C}$ als $\mathbb{R}$-lin deelruimte

$X^2 + bX + c$ is irred. desda het geen nulp. in $\mathbb{R}$
heeft, desda $(X + \frac{1}{2}b)^2 - (\frac{1}{4}b^2 - c)$ geen nulp. in $\mathbb{R}$
heeft, desda $\frac{1}{4}b^2 - c$ geen wortel in $\mathbb{R}$
heeft, desda $\frac{1}{4}b^2 - c < 0$ desda $b^2 - 4c < 0$ $\boxtimes$

def Een algebraïsche afsluiting van lich K
is een uitbreiding $K \subset \overline{K}$ met

1. $\overline{K}$ is algebraïsch over K
2. $\overline{K}$ is algebraïsch afgesloten.

— niet te verwarren met de definitie na 10.8 :

def zij $L \supset K$ uitbr. van lichamen.

de verz. $\{ \alpha \in L : \alpha$ algebr. over $K \}$ is
een deellichaam van L dat K omvat
en dit noemt men ook wel de algebraïsche
afsluiting van K in L

Vbd $\mathbb{C}$ is een algbr. afsluiting van $\mathbb{R}$.

Stell. 13.12 $\mathbb{Q}$ heeft een algebraïsche afsluiting

bew Zij $\overline{\mathbb{Q}}$ de algebr. afsl. van $\mathbb{Q}$ in $\mathbb{C}$, ie

$$\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} : \alpha \text{ is algebraïsch over } \mathbb{Q} \}$$

Dit is een per definitie en 10.8 (stelling: ~~het is een lichaam~~) algebraïsche lichaamsuitbr. van $\mathbb{Q}$. We hoeven alleen te laten zien dat $\overline{\mathbb{Q}}$ algebraïsch afgesloten is.

Zij $f \in \overline{\mathbb{Q}}[X]$ niet-constant. Omdat $f \in \mathbb{C}[X]$ heeft f een np., zeg α in $\mathbb{C}$. We moeten aantonen: $\alpha \in \overline{\mathbb{Q}}$

$\overline{\mathbb{Q}}(\alpha)$ is algebraïsch over $\overline{\mathbb{Q}}$ want $f \in \overline{\mathbb{Q}}[X]$ heeft nulpunt α (definitie) en $\overline{\mathbb{Q}}$ is per constructie algebraïsch over $\mathbb{Q}$, dus $\overline{\mathbb{Q}}(\alpha)$ is algebraïsch over $\mathbb{Q}$, per stelling 10.9

Ihb is $\alpha \in \overline{\mathbb{Q}}(\alpha)$ algebr. over $\mathbb{Q}$, dus $\alpha \in \overline{\mathbb{Q}}$ per definitie $\Rightarrow f$ bevat np. in $\overline{\mathbb{Q}}$

Dus $\overline{\mathbb{Q}}$ is alg. afgesloten $\square$

Met hetzelfde argument zien we Iha dat Als $K \subset L$ uitbr en $L \subset \overline{L}$ een alg. afsluiting is (in ons geval $\mathbb{Q} = K$, $L = \overline{L} = \mathbb{C}$) dan is

$$\overline{K} = \{ \alpha \in \overline{L} : \alpha \text{ algbr. over } K \}$$

een alg. afsluiting van K:

$f \in \overline{K}[X]$ niet-const dan $f \in \overline{L}[X]$ dus heeft np $\alpha \in \overline{L}$ en $\overline{K}(\alpha)$ is alg. over $\overline{K}$ (want eindig), $\overline{K}$ alg. over K (per constructie) $\xRightarrow[10.9]{} \overline{K}(\alpha)$ alg. over K dus $\alpha \in \overline{K}$

$\square$

— Om na te gaan of een uitbr. $K \subset L$ een alg. afsluiting is, blijkt het voldoende om een eigenschap na te gaan die op eerste gezicht zwakker lijkt dan de voorwaarden in def. of 13.2

— Lemma: Zij $K \subset L$ een algebraische uitbreiding van lichamen (bijv. niet $\mathbb{Q} \subset \mathbb{R}$)

Én zodat elk niet-const. $f \in K[X]$ in $L[X]$ splijt in lineaire factoren. Dan is L een alg. afsl. van K.

Bew L is alg. over K, dus we hoeven alleen nog na te gaan dat L algebraisch afgesl. is.

let goed op:

Aanname: elke $f \in K[X] - K$ splijt in $L[X]$

T.B elke $f \in L[X] - L$ splijt in $L[X]$

Neem dus $g \in L[X] - L$. Zij $L \subset M = \Omega^g_L$ (later blijkt dat $M = L$, maar dat weten we nu nog niet. Net zoals in 13.8 dat later zal blijken $\Omega^f_{\mathbb{C}} = \mathbb{C}$ in lemma 13.8)

Zij $\alpha \in M$ een nulpunt van g, en laat $f = f^\alpha_K$. Dit bestaat, omdat α algebraisch over L is en L alg. over K.

Bovendien is de uitbr. graad van $K(\alpha)$ in K groter of zo groot als die van $L(\alpha)$ in α, omdat $K \subset L$ dus min polynoom f^α_K ligt ook in $L[X]$ dus f^α_K heeft minstens zo'n grote graad als f_L^α, omdat anders f_L^α niet minimum is, want dan kan f_K^α als min pol. dienen.

$\Rightarrow$ $f = f_K^\alpha \in L[X]$ wordt gedeeld door $g \in L[X]$ want $f(\alpha) = 0$

Maar anderzijds splijt f in $L[X]$ in lin. factoren, dus wegens unic. van priemontb in $L[X]$ (HIR $\Rightarrow$ UFD) g ook
$\Rightarrow$ g splijt in $L[X]$ in lin. factoren $\square$

Bovenstaand lemma is directe generalisatie van:

— Als elke $f \in \mathbb{R}[X]$ n.p. in $\mathbb{C}$ heeft, dan is $\mathbb{C}$ alg. afsluiting van K dus alg. gesloten.