Velduitbreidingen

Hector Mommaerts

Hoofdstuk 1

Basisbegrippen

1.1 Definities

Definitie 1.1. Een veld L is een uitbreiding van het veld K als het ontstaat door aan K één of meerdere elementen toe te voegen.
Notatie: $L|K$

Definitie 1.2. De graad van $L|K$ is de dimensie van L als vectorruimte over K. Notatie: $[L : K]$

Enkele opmerkingen:

- L is een uitbreiding van graad 1 van K als en slechts als $L = K$.
- Als we aan het veld K een element a toevoegen, dan noteren we dze velduitbreiding met $K(a)$. Het is het kleinst mogelijke veld rond K dat a bevat. We spreken dan van een *enkelvoudige uitbreiding* en we noemen a het *primitief of voortbrengend* element van de uitbreiding.
- Een uitbreiding van graad 2 noemen we een *kwadratische uitbreiding* .
- Een uitbreiding van graad 3 noemen we een *kubische uitbreiding* .
- Een eindige uitbreiding van $\mathbb{Q}$ noemen we een *algebrïsch getallenveld*.

- Als L een velduitbreiding is van K en M is een uitbreiding van L, dan is M ook een uitbreiding van K en $[M : K] = [M : L] . [L : K]$. We noemen L een *tussenveld*.

- Als L een uitbreiding is van K, dan noemen we een element $\alpha \in L$ *algebraïsch* als het de wortel is van een niet-nul, monische veelterm met coëfficiënten in K. Een element dat niet algebraïsch is, noemen we *transcendent* .

1.2 Voorbeelden

- $\mathbb{R}|\mathbb{Q}$ is een velduitbreiding met oneindige graad.

- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is een kwadratische uitbreiding van $\mathbb{Q}$.

- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$ is een uitbreiding van $\mathbb{Q}$ met graad 4. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is ook een kwadratische uitbreiding van $\mathbb{Q}(\sqrt{2})$. Maar bovendien is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ een enkelvoudige uitbreiding van $\mathbb{Q}$ want $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \{a+b(\sqrt{2}+\sqrt{3})+c(\sqrt{2}+\sqrt{3})^2+ d(\sqrt{2}+\sqrt{3})^3 : a, b, c, d \in \mathbb{Q}\}$.

- $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ is een kwadratische uitbreiding van $\mathbb{Q}$.

Hoofdstuk 2

Ontbindingsvelden

2.1 Definities

Definitie 2.1. Een ontbindingsveld van een veelterm $P(X)$ over een veld K is een velduitbreiding L van K waarin $P(X)$ ontbonden kan worden in allemaal lineaire factoren.

Enkele opmerkingen:

- De wortels van $P(x)$ genereren L over K.
- Dergelijke ontbindingsvelden bestaan en zijn uniek op een isomorfisme na.
- Een ontbindingsveld van een veelterm $P(X)$ over K is steeds een eindige uitbreiding en is dus in het bijzonder steeds een algebraïsche velduitbreiding van K.

Hoe construeren we een ontbindingsveld L van een veelterm $P(X)$ over K van graad n?
De algemene procedure is het construeren van een rij van velden
$K = K_0, K_1, \cdots, K_{i-1}, K_i, \cdots K_r = L$, waarbij elke K_i een velduitbreiding is van K_{i-1} die ontstaat door een nieuwe wortel van $P(X)$ toe te voegen. Omdat $P(X)$ hoogstens n wortels heeft, zullen we hoogstens n uitbreidingen hebben

1. Ontbind $P(X)$ in irreducibele factoren :$P_1(X).P_2(X).\cdots.P_k(X)$.

2. Neem een willekeurige factor $P_i(X)$ die niet van de eerste graad is.

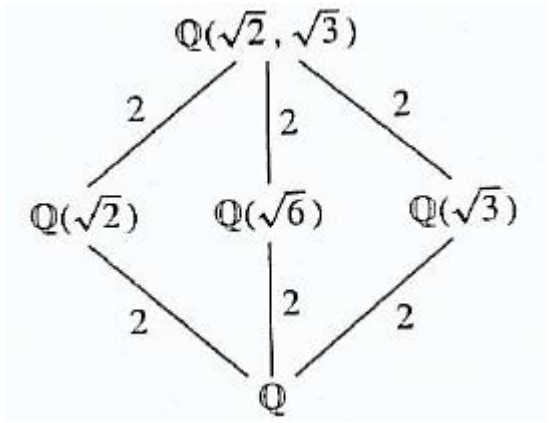
3. Bepaal de velduitbreiding K_i van K_{i-1} als $\frac{K_{i-1}[X]}{(P_i(X))}$. Hierbij is $(P_i(X))$ het ideaal van $K_{i-1}[X]$ voortgebracht door $(P_i(X))$.

4. Herhaal dit proces voor alle niet-lineaire factoren van $P(X)$.

2.2 Voorbeelden

- Neem de veelterm $P(X) = X^2 - 2 \in \mathbb{Q}[X]$. Het onbindingsveld van $P(X)$ is $\mathbb{Q}(\sqrt{2})$. De veelterm $P(X)$ is irreducibel in $\mathbb{Q}[X]$. Construeer $K_1 = \frac{\mathbb{Q}[X]}{(X^2-2)}$. We zien dat $\mathbb{Q}(\sqrt{2})$ isomorf is met $\frac{\mathbb{Q}[X]}{(X^2-2)}$, via $f(a+b\sqrt{2}) = a+bX$. Want $(a+bX).(c+dX) = ac+bdX^2+(ad+bc)X \equiv ac + 2bd + (ad + bc)X \bmod (X^2 - 2)$. En $f((a + b\sqrt{2})(c + d\sqrt{2})) = f(ac + 2bd + (ad + bc)\sqrt{2} = ac + 2bd + (ad + bc)X$.

- Het ontbindingsveld van $P(X) = (X^2 - 2)(X^2 - 3)$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dit is een uitbreiding van graad 4 over $\mathbb{Q}$



- Neem $P(X) = x^3 - 2$. De wortels van deze vergelijking zijn $\sqrt[3]{2}, \sqrt[3]{2}\omega$ en $\sqrt[3]{2}\omega^2$, waarbij $\omega = \frac{-1-\sqrt{3}i}{2}$ en $\omega^2 = -1 - \omega$. Omdat $\sqrt[3]{2}\omega^2 = -\sqrt[3]{2} - \sqrt[3]{2}\omega$ zal de derde wortel van de vergelijking gelegen zijn in het ontbindingsveld dat de twee eerste wortels bevat. Het gezochte ontbindingsveld is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$. Met de hierboven gegeven constructie geeft dat: $K_0 = \mathbb{Q}$ en $K_1 = \frac{\mathbb{Q}[X]}{(X^2+3)}$. Dit veld is isomorf met $\mathbb{Q}(\sqrt{3}i)$

via $f(a + b\sqrt{3}i) = a + bX$ en is dus een velduitbreiding van graad 2. Definieer vervolgens $K_2 = \dfrac{K_1[X]}{(X^3 - 2)}$. Dit veld is isomorf met $K_1(\sqrt[3]{2})$ via $f(a + b\sqrt[3]{2} + \sqrt[3]{2}^2) = a + bX + cX^2$ en is dus een velduitbreiding van graad 3. Bijgevolg is K_2 een velduitbreiding van $\mathbb{Q}$ van graad 6.

Hoofdstuk 3

Galois groep van een velduitbreiding

3.1 Definities

Definitie 3.1. Zij $L|K$ een velduitbreiding. Een *K-automorfisme van L* is een automorfisme van L dat alle elementen van K fixeert.

Definitie 3.2. Zij $L|K$ een velduitbreiding. De verzameling van alle K-automorfsmen van L vormt een groep onder de samenstelling, die we de *Galoisgroep van de velduitbreiding* $L|K$ noemen, en noteren als $Gal(L|K)$.

Definitie 3.3. Zij K een willekeurig veld en H een deelgroep van $Aut(K)$. Dan is $Fix(H) = \{x \in K : \sigma(x) = x \ : \forall \sigma \in H\}$

Definitie 3.4. Zij $L|K$ een velduitbreiding. We noemen $L|K$ een *Galois uitbreiding* als $L|K$ eindig is en $Fix(Gal(L|K)) = K$.

Enkele belangrijke resultaten:

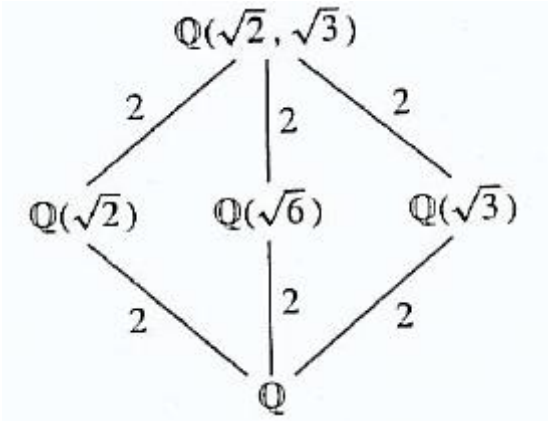
- Een eindige velduitbreiding $L|K$ een Galois uitbreiding is als en slects als L het ontbindingsveld is van een veelterm f in $K[X]$, zodat elke irreducibele factor van f in $K[X]$ geen meervoudige wortels heeft.
- Er is een nauw verband tussen de graad van een velduitbreiding en de orde van de corresponderende Galoisgroep: het aantal elementen in de Galoisgroep is altijd een deler van de graad van de velduitbreiding en het is er gelijk aan als en slechts als de velduitbreiding een Galois uitbreiding is.
- Er is een bijectief verband tussen de deelgroepen van de Galois groep en de tussenliggende velden van de velduitbreiding.
- Eigenschappen van de Galois groep van een velduitbreiding, worden overgedragen op de velduitbreiding. We noemen, bijvoorbeeld, een velduitbreiding cyclisch als zijn Galois groep een cyclische groep is.

3.2 Voorbeelden

- De velduitbreiding $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is een Galois uitbreiding. De elementen van de Galois groep zijn de identieke transformatie en de transformatie die $\sqrt{2}$ afbeeldt op $-\sqrt{2}$. Deze groep is isomorf met C_2. De Galois groep heeft dus geen echte deelgroepen en er zijn dus geen tussenvelden bij de velduitbreiding.
- De velduitbreiding $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ is een Galois uitbreiding, dus heeft de Galois groep van de uitbreiding evenveel elementen als de graad van de velduitbreiding, die gelijk is aan 4. De elementen van de Galois groep zijn bepaald door de beelden van $\sqrt{2}$ en $\sqrt{3}$.

$\sigma(\sqrt{2})$	$\sigma(\sqrt{3})$
$\sqrt{2}$	$\sqrt{3}$
$\sqrt{2}$	$-\sqrt{3}$
$-\sqrt{2}$	$\sqrt{3}$
$-\sqrt{2}$	$-\sqrt{3}$

  Elk automorfisme heeft orde 2, dus is $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}) \cong C_2 \times C_2$, de groep van Klein. De Galois groep heeft 3 normaaldelers met twee elementen en dus heeft de velduitbreiding 3 tussenvelden K_i zodat $\left[\mathbb{Q}(\sqrt{2},\sqrt{3})|K_i\right] = 2$ en $[K_i|\mathbb{Q}] = \frac{4}{2} = 2$.


$\mathbb{Q}(\sqrt{2},\sqrt{3})$
2
2
2
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{6})$
$\mathbb{Q}(\sqrt{3})$
2
2
2
$\mathbb{Q}$