

GALOISGRUPPER

OSCAR MARMON

Låt $K \subseteq L$ vara en kroppsutvidgning. $\text{Aut}(L)$ = gruppen av automorfier på L , dvs isomorfier $L \rightarrow L$. Vi definierar *Galoisgruppen* för utvidgningen:

$$\text{Gal}(L/K) = \{\sigma \in \text{Aut}(L); \sigma(a) = a \forall a \in K\},$$

en delgrupp av $\text{Aut}(L)$.

Exempel. $\mathbb{R} \subseteq \mathbb{C}$. Låt $G = \text{Gal}(\mathbb{C}/\mathbb{R})$. $\mathbb{C} = \mathbb{R} + \mathbb{R}i$, så $\sigma \in G$ bestäms entydigt av $\sigma(i)$. Vi har

$$\begin{aligned} -1 &= \sigma(-1) = \sigma(i^2) = \sigma(i)^2 \\ &\implies \sigma(i) = \pm i. \end{aligned}$$

Alltså är $G = \{\sigma_1, \sigma_2\}$, där $\sigma_1 : i \mapsto i$ och $\sigma_2 : i \mapsto -i$.

ALGEBRAISKA UTVIDGNINGAR

I en kroppsutvidgning $K \subseteq L$ kallas ett element $\alpha \in L$ *algebraiskt över K* om det finns $f(X) \in K[X]$ s.a. $f(\alpha) = 0$. Kroppsutvidgningen kallas *algebraisk* om alla $\alpha \in L$ är algebraiska över K . Vi är bara intresserade av Galoisgrupper för algebraiska utvidgningar $K \subseteq L$. *Minimalpolynomet* för $\alpha \in L$ över K , $\min_K(\alpha)$ = det unika irreducibla moniska polynom över K som har α som nollställe.

Anmärkning. Om $\sigma \in \text{Gal}(L/K)$ och $\alpha \in L$ är ett nollställe till $f(X) \in K[X]$ så är trivialt även $\sigma(\alpha)$ ett nollställe till $f(X)$.

Exempel (Ändliga kroppar). Varje ändlig kropp K har kardinalitet p^n för något primtal p , och har kroppen \mathbb{F}_p med p element som delkropp. $K = \mathbb{F}_{p^n}$ genereras över \mathbb{F}_p av samtliga nollställen till polynomet $X^{p^n} - X \in \mathbb{F}_p[X]$.

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$$

och genereras av *Frobeniusautomorfin* $\sigma : \alpha \rightarrow \alpha^p$.

För varje delgrupp $H \subseteq \text{Aut}(L)$ kan vi definiera delkroppen

$$\text{Fix}(H) = \{\alpha \in L; \sigma(\alpha) = \alpha \forall \sigma \in H\}.$$

För att Galoisteorin ska fungera bra vill vi att $\text{Fix}(\text{Gal}(L/K)) = K$. Detta är fallet om vi har en *Galoisutvidgning*.

Definition. En algebraisk utvidgning $K \subseteq L$ kallas *Galois* om den är *normal* och *separabel*.

Normalitet. $K \subseteq L$ är *normal* om $\min_K(\alpha)$ sönderfaller i linjära faktorer för varje $\alpha \in L$.

Exempel. $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}]$ är inte normal, ty de två komplexa nollställena till $X^3 - 2$ finns ej med.

Separabilitet. En utvidgning $K \subseteq L$ är *separabel* om för varje $\alpha \in L$ $\min_K(\alpha)$ saknar multipla nollställen.

Exempel. $\mathbb{F}_p =$ kroppen med p element, p primtal. $K = \mathbb{F}_p(T)$, kroppen av rationella funktioner i variabeln T . $L = K[\alpha]$, där α är ett nollställe till $f(X) = X^p - T \in K[X]$.

$$f(X) = X^p - T = X^p - \alpha^p = (X - \alpha)^p$$

Alltså är α ett multipelt nollställe, och $K \subseteq L$ ej separabel.

Om $\text{kar}(K) = 0$ eller K är ändlig, så är varje utvidgning $K \subseteq L$ separabel.

GALOISKORRESPONDENSEN

En kroppsutvidgning $K \subseteq L$ är *ändlig* om dimensionen av L som vektorrum över K är ändlig. Denna dimension betecknas då $\deg_K L$, *graden* av utvidgningen.

Sats (Galoisteorins huvudsats(G.H.)). $K \subseteq L$ ändlig Galoisutvidgning. $G = \text{Gal}(L/K)$. Låt

$$\mathcal{F} = \{F; K \subseteq F \subseteq L\},$$

$$\mathcal{G} = \{H; H \subseteq G\}.$$

Då finns bijektiv motsvarighet mellan \mathcal{F} och \mathcal{G} , som ges av

$$\begin{array}{ccc} g : \mathcal{F} \rightarrow \mathcal{G} & & f : \mathcal{G} \rightarrow \mathcal{F} \\ F \mapsto \text{Gal}(L/F) & & H \mapsto \text{Fix}(H) \end{array}$$

Obs:

$$F_1 \subseteq F_2 \Rightarrow g(F_1) \supseteq g(F_2)$$

och vice versa. Vi har

$$[G : \text{Gal}(L/F)] = \deg_K F.$$

Vidare är $\text{Gal}(L/F) \trianglelefteq \text{Gal}(L/E)$ omm $E \subseteq F$ är Galois, och i så fall har vi

$$\text{Gal}(F/E) \simeq \text{Gal}(L/E)/\text{Gal}(L/F).$$

Om $K \subseteq L$ är oändlig har vi ej nödvändigtvis $\text{Gal}(L/\text{Fix}(H)) = H$ (men självklart " \supseteq ").

Exempel (Cirkeldelningskroppar). $F_n = \mathbb{Q}[\zeta_n]$, där $\zeta_n = e^{2\pi i/n}$, kallas den n :te cirkeldelningskroppen eller cyklotomiska kroppen.

$$\deg_{\mathbb{Q}} F_n = \varphi(n) = \#\{1 \leq m \leq n; \text{sgd}(m, n) = 1\}.$$

$$\text{Gal}(F_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

(vi kan skicka ζ_n på vilken som helst av de primitiva n :te enhetsrötterna $e^{2\pi im/n}$, $\text{sgd}(m, n) = 1$.) Om $m \mid n$ har vi $F_m \subseteq F_n$. Vi får (G.H.) en surjektiv avbildning

$$\text{Gal}(F_n/\mathbb{Q}) \rightarrow \text{Gal}(F_m/\mathbb{Q})$$

som sammanfaller med den kanoniska $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$.

OÄNDLIGA UTVIDGNINGAR. KRULLTOPOLOGIN

$K \subseteq L$ (oändlig) Galoisutvidgning, $G = \text{Gal}(L/K)$. Låt \mathfrak{N} vara familjen av delgrupper $\text{Gal}(L/F)$ där $K \subseteq F$ är ändlig ($\Rightarrow \text{Gal}(L/F)$ oändlig). Vi kan göra G till en topologisk grupp genom att införa *Krulltopologin*, där vi tar \mathfrak{N} som bas av omgivningar till identiteten.

Sats. G med Krulltopologin är kompakt, Hausdorff och totalt osammanhängande (varje sammanhängande komponent är en punkt).

Nu har vi följande samband:

$$\text{Gal}(L/\text{Fix}(H)) = \overline{H}.$$

Vi får en utvidgning av Galoisteorins huvudsats:

Sats. $K \subseteq L$ Galois. Avbildningen från G.H. ger en bijektiv motsvarighet mellan slutna delgrupper av $\text{Gal}(L/K)$ och delkroppar $K \subseteq F \subseteq L$.

Låt \mathcal{F} vara mängden av mellanliggande delkroppar $K \subseteq F \subseteq L$ där $K \subseteq F$ är ändlig och normal. Vi får ett *inverst system* av topologiska grupper $\text{Gal}(F/K)$, $F \in \mathcal{F}$, ty om $F \subseteq F'$ har vi en avbildning

$$\text{Gal}(F'/K) \rightarrow \text{Gal}(F'/K)/\text{Gal}(F'/F) \simeq \text{Gal}(F/K).$$

Sats. $\text{Gal}(L/K) \simeq \varprojlim_{F \in \mathcal{F}} \text{Gal}(F/K)$.