FFC 14.5.08

Abzählen d. surj. $\mathbb{F}_q$-Homom. $\varphi: V \to W$ analog

zu Abzählen d. surj Abb. zw. endl. Mengen. (Möbius Inversion)

Sei V n-dim, W m-dim $\mathbb{F}_q$-VR U ein Teilraum $\leq W$.

$g(U) = \#\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(V,W) \mid \mathrm{Im}\,\varphi \subseteq U\}$

$f(U) = \#\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(V,W) \mid \mathrm{Im}\,\varphi = U\}$

$g(U) = |\mathrm{Hom}_{\mathbb{F}_q}(V,U)| = q^{n(\dim U)}$

Es gilt $g(U) = \sum_{A \leq U} f(A)$. mit Möbius Inversion: $f(U) = \sum_{A \leq U} \mu(A,U) \cdot g(A)$

$= \sum_{A \leq U} (-1)^{\dim U/A} \cdot q^{\binom{\dim U/A}{2}} q^{n \cdot \dim A} = \sum_{j=0}^{\ell} (-1)^{\ell-j} \begin{bmatrix} \ell \\ j \end{bmatrix}_q q^{\binom{\ell-j}{2} n \cdot j}$

surj $\mathbb{F}_q$-Hom $V \to W = f(W)$ $(\dim W = m)$

$= \sum_{k=0}^{m} \begin{bmatrix} m \\ k \end{bmatrix}_q (-1)^{m-k} q^{\binom{m-k}{2} + n \cdot k} = \sum_{k=0}^{m} \begin{bmatrix} m \\ k \end{bmatrix}_q (-1)^k q^{\binom{k}{2} + n(m-k)}$

Korolar: $\#(n \times m)$ Matrizen über $\mathbb{F}_q$ vom Rang $\ell = \begin{bmatrix} m \\ \ell \end{bmatrix}_p \cdot \sum_{j=0}^{\ell} (-1)^{\ell-j} \begin{bmatrix} \ell \\ j \end{bmatrix}_q q^{\binom{\ell-j}{2} + n \cdot j}$

Galois-Theorie

Der „triviale Anteil" an Hauptsatz d. Galois-Theorie besteht an folgenden Tatsachen über „Galois-Korrespondenzen".

Def: Eine Galois-Korrespondenz ~~besteht~~ besteht aus zwei halb geord. Mgn $(X, \leq), (Y, \leq)$ mit Abbildungen $\varphi: X \to Y$ $\psi: Y \to X$ die folgende Bedingungen erfüllen: Da die Bed. symmetr. in φ, ψ sind schreibe wir a' für $\varphi(a)$ bzw $\psi(a)$ jenachdem ob $a \in X$ od $a \in Y$ $\quad a' \leftarrow a$, $b \mapsto b'$

(i) $a \leq b \Rightarrow b' \leq a'$

(ii) $a \leq a''$

Bsp: O Menge von Objekte, E Menge von Eigenschaften

(z.B Bücher in Bibliothek, Schlagworte in Katalog)

$X = (\mathcal{P}(O), \subseteq)$ $(Y = \mathcal{P}(E), \subseteq)$

$A \subseteq O \quad A \mapsto A' = \{e \in E \mid \forall a \in A \text{ hat } E_i\ e\}$

$B \subseteq E \quad B \mapsto B' = \{a \in O \mid \forall b \in B \text{ } b \text{ hat } E_i\}$

Bsp: $\mathcal{O} = K[x_1 .. x_n]$, $E = K^n$ Galois Korrespondenz zw $\mathcal{P}(\mathcal{O}), \mathcal{P}(K^n)$ gg durch $A \subseteq K[x_1 .. x_n] \mapsto Z(A) = A' = \{b \in K^n \mid \forall f \in A \quad f(b) = 0\}$

$B \subseteq K^n \mapsto J(B) = B' = \{f \in K[x_1 .. x_n] \mid \forall b \in B \quad f(b) = 0\}$

Lemma: Wenn zwischen $(X, \leq)$ $(Y, \leq)$ eine Galois-Korrespondenz $x \mapsto x'$ besteht, dann:

(III) $a''' = a'$

(IV) äquivalent ist $a'' = a$ und $\exists b : a = b'$ || Not: die Elemente $a'' = a$ heißen Galois-abgeschl.

(V) Bijektion zw allen Galois-Abgeschl. El von X und allen Galois-abg El von Y gegeben durch (Einschränkung von) $x \mapsto x'$

Die Galois-Korrespondenz die die Theorie ihren Namen gegeben hat ist:

für einen Körper zwischen $K \subseteq F$ sei X = Menge der Zwischenkörper $= \{L \mid L \text{ Körper } K \subseteq L \subseteq F\}$

und $G = \mathrm{Aut}_K F = \{\sigma \in \mathrm{Aut}\, F \mid \forall k \in K \; \sigma(k) = k\}$

$Y = \{$ Menge der Untergruppen von $G\}$ (X, Y durch $\subseteq$ geordnet) mit der

Korrespondenz Körper $L \mapsto L' = \{\sigma \in G \mid \forall l \in L \; \sigma(l) = l\} \leq G$

$H \leq G$, $H \mapsto H'$ (Fix Körper von H) $= \{a \in F \mid \forall \sigma \in H \; \sigma(a) = a\}$

$$= \bigcap_{\sigma \in H} \mathrm{Fix}\,\sigma \leq F \qquad K \subseteq F' \subseteq L$$

Def: Nennen Körper-Erw $F:K$ eine Galois-Erw, wenn $G' = K$, d.h. wenn $(\mathrm{Aut}_K F)' = K$ (die Gruppe der K-Automorphismen von F hat als Fixkörper nur K, nicht einen größeren Körper $K'' \supsetneq K$.

$(\mathrm{id})' = F$ $\qquad \{\mathrm{id}\} = F' \quad (\mathrm{id})'' = F''' = F' = \{\mathrm{id}\}$

$F'' \{\mathrm{id}\}'' = \{\mathrm{id}\}'$ $\quad L \mapsto L'$

$K'' = G'$ $\quad H' \leftarrow H$

$K \leftarrow G = \mathrm{Aut}_K F \qquad G'' = K''' = K' = G$

Es sind $F, \{\mathrm{id}\}, G = \mathrm{Aut}_K F$ immer Galois abgeschlossen. Es kann $G' = K'' \supsetneq K$ sein.

Galois: $\Leftrightarrow K'' = K$.

Anderer Zugang zur Galois-Theorie startet mit Körper F und Gruppe $G \leq \mathrm{Aut}\, F$, setzt $K := \mathrm{Fix}\, G = \bigcap_{g \in G} \mathrm{Fix}\, g$ der $F:K$ Galois Erw.

Hauptsatz der Galois-Theorie

$F:K$ endl. die Galois-Erweiterung (d.h. $K = \mathrm{Fix}_{\mathrm{Körper}}$ von $\mathrm{Aut}_K F$) dann ist durch

$L \mapsto L' = \{\sigma \in \mathrm{Aut}_K F \mid \forall l \in L\ \sigma(l) = l\}$ für L Körper mit $K \subseteq L \subseteq F$ und

$H \mapsto H' = \{a \in F \mid \forall \sigma \in H\ \sigma(a) = a\}$ für $H \leq \mathrm{Aut}_K F$ eine Bijektion zw.

alle Zwischenkörper L ($K \subseteq L \subseteq F$) und allen Untergruppen von $\mathrm{Aut}_K F$ geg.,

und $[A:B] = [B':A']$ für alle A, B Zwischenkörper von $F:K$ bzw A, B

Ugr von $\mathrm{Aut}_K F$. [Ws. Bijektion zwischen Galois-abg. Elementen ein

Galois-Koresp. genaueres 28. alle Zwischenkörper, alle Ugr sind Galois-abg: $A'' = A$]

Ü: ~~XX~~, $F:K$ endl Körper $\Rightarrow$ $F:K$ Galois (Fortsetzbarkeit von Isom. auf

ein fach Erw.)

Vorschau: Es gilt für algebraische Körpererweiterung $F:K$

$F:K$ Galois $\Leftrightarrow$ $F:K$ separabel & normal

$\Leftrightarrow$ $F:K$ separabel & F Zerf.kö über K einer Menge von Poly $\subseteq K[x]$

Daher für perfekten Körper K (insb. endl Körper und solche mit $\chi(K) = 0$)

gilt $F:K$ alg $\Rightarrow$ ($F:K$ Galois $\Leftrightarrow$ $F:K$ Zerf.kö)

Bem: $\sigma \in \overset{\text{End}}{\cancel{\text{Aut}}} F$, $K \subseteq F$, $f \in K[x]$; wenn σ die Elem von K elementweise

fix lässt, dann bildet σ Nullstelle von f auf Nullstelle von f ab:

$u \in F$ mit $f(u) = 0$ dann $f(\sigma(u)) = \sigma(f(u)) = \sigma(0) = 0$

$f(\sigma(u)) = \sigma(f(u))$ weil, wenn $f = \sum_k a_k x^k$ $a_k \in K$ dann

$\sigma(f(u)) = \sigma(\sum a_k u^k) = \sum \sigma(a_k)\, \sigma(u)^k = \sum a_k \sigma(u)^k = f(\sigma(u))$.

Insb. wenn $\sigma \in \mathrm{Aut}\, F$ dann ~~folgt~~ permutiert σ die Nst von f in F

Lemma: $F:K$ ~~endl~~ Körpererw $F \supseteq M \supseteq L \supseteq K$. $M:L$ Zwischenkörper mit $[M:L]$ endl. $\Rightarrow$

$[L':M']$ (endl) $\leq [M:L]$.

Kor: $[F:K]$ endl dim $\Rightarrow$ $|\mathrm{Aut}_K F| \leq [F:K]$

Beweis: zuerst Spezialfall einf. algebraische Erw: $M = L[u]$

$L' = \overset{F}{\cancel{\text{Aut}}}_L = \mathrm{Aut}_L F$, $M' = \mathrm{Aut}_M F = \{\sigma \in \mathrm{Aut}_L F \mid \sigma(u) = u\} = St_{\mathrm{Aut}_L F}(u)$

$[L':M'] = [\mathrm{Aut}_L F : St_{\mathrm{Aut}_L F}(u)] = \#$ Li-Nk von $St(u)$ in $\mathrm{Aut}_L F$

$\exists$ Bijektion zw. Li-Nk von $St(u)$ in $\mathrm{Aut}_L F$ und dem Orbit von u unter

$\mathrm{Aut}_L F$. d.h. die Menge der Bilder $\sigma(u)$, $\sigma \in \mathrm{Aut}_L F$

Da v alg über L, v Nullst. sein Minimalp. $f \in L[X]$ über K, alle $\sigma(u)$ mit $\sigma \in \mathrm{Aut}_L F$ sind auch Nst. von f von denen es ganau $[L(u):L]$ viele gibt: also $[L':M'] \leq [L(u):L] = [M:L]$.

Allgemeine Fall: Ind ^{v} $[M:L]$: $[M:L]=1 \Rightarrow M=L \Rightarrow M'=L'$

$n = [M:L] > 1$ wähle $v \in M \setminus L$, wenn $M = L(u)$ fertig,

sonst
M — $\mathrm{Aut}_M F = M'$
$L(u)$ — $\mathrm{Aut}_{L(u)} F = L(u)'$
L — $\mathrm{Aut}_L F = L'$

Nach IV $[L':L(u)'] \leq [L(u):L]$
und $[L(v)':M'] \leq [M:L(v)]$
insg: $[L':M'] = [L':L(u)'] \cdot [L(u)':M'] \leq$
$\leq [L(u):L] \cdot [M:L(v)] = [M:L]$ ✓

Ü: (nach vorigen Ü gilt für K, F all. $F:K$ Galois)
$\mathrm{Aut}_K F$ erzeugt von φ, $\varphi(x) = x^q$, $|K| = q$.