7.10 Satz Sei $K \subset L$ ein Unterkörper eines algebraisch abgeschlossenen Körpers L. Dann ist ~~der algebraische Abschluss~~

$$\bar{K}^L = \{ a \in L \mid a \text{ ist algebraisch über } K \}$$

ein algebraisch abgeschlossener Körper.

Beweis Sei $f \in \bar{K}^L[x]$ ein nicht konstantes Polynom, etwa $f = x^n + c_1 x^{n-1} + \dots + c_n$, dann sind die Koeffizienten c_i algebraisch über K. Ist nun $a \in L$ eine Nullstelle von f, dann ist a algebraisch über $K[c_1, \dots, c_n]$ und

$$[K[c_1, \dots, c_n, a] : K] < \infty$$

$\Rightarrow a$ ist algebraisch über K

$\Rightarrow a \in \bar{K}^L$ $\square$

Mit $\bar{\mathbb{Q}} \subset \mathbb{C}$ bezeichnen wir $\bar{\mathbb{Q}}^{\mathbb{C}}$ den algebr. Abschl. von $\mathbb{Q}$ in $\mathbb{C}$.

$\mathbb{Q} \subset \bar{\mathbb{Q}}$ ist eine alg. Körpererweiterung und

$$[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty, \text{ da } \bar{\mathbb{Q}} \supset \mathbb{Q}[\sqrt[n]{p}]$$

$[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = n$ beliebig groß gewählt werden kann.

7.12 Satz (Kroneckers Trick)

Sei K ein bel. Körper und $f \in K[x]$ ein nicht konstantes Polynom. Dann gibt es einen Oberkörper L in dem f eine Nullstelle hat.

Beweis: Wir dürfen f durch einen irreduziblen Faktor ersetzen und betrachten dann $L = K[x]/(f)$

Da f irreduzibel ist, ist L ein Körper.

Sei $\bar{x}$ ~~$= x+(f) \in$~~ $\in L$ die Klasse $x + (f) \in K[x]/(f)$.

Dann gilt $f(\bar{x}) = f(x + (f)) = f(x) + (f)$

$$= f + (f) = (f) = 0 \in \frac{K[x]}{(f)} = L$$

Also $\bar{x}$ ist eine Nullstelle von f in L

7.13 Satz Sei K Körper, $f \in K[x]$ nicht konstant. Dann existiert ein Oberkörper $L \supset K$ sodass $f \in L[x]$ in Linearfaktoren zerfällt.

Beweis Induktion nach $n = \deg f$.
Im Fall $n = 1$ ist $L = K$ so ein Körper
Sei nun $n > 1$ und $L_1 \supset K$ ein Oberkörper, in dem f eine Nullstelle $a_1 \in L$ hat. Dann gilt

$$f = (x - a_1) f_1 \quad \text{wobei } \deg f_1 < \deg f \text{ und } f_1 \in L_1[x]$$

Nach IV existiert ein Oberkörper $L \supset L_1 \supset K$ über dem f_1 zerfällt also auch f zerfällt $\square$

7.14 Def Sei $f \in K[x]$ ein nicht konstanter Polynom und $L \supset K$ ein Oberkörper über dem f in Linearfaktoren zerfällt etwa $f = \lambda \cdot \prod_{i=1}^{n} (x - a_i)$ wobei $\lambda \in K$ der Leitkoeffizient ist. Dann ist

$$K[a_1, \ldots, a_n] \subset L$$ der kleinste ~~Körper~~ ~~umfa~~ K umfassende Unterkörper von L in dem f in Linearfaktoren zerfällt. $K[a_1, \ldots, a_n]$ nennt man einen Zerfällungskörper von f

7.15 Satz Sei $f \in K[x]$ nicht konstant vom Grad n. Je zwei Zerfällungskörper

$$K[a_1, \ldots, a_n] = K[a_1', \ldots, a_n']$$

sind isomorph.

Beweis: Wir zeigen: Bei geeigneter Nummerierung von $a_1', \ldots, a_n'$ lässt sich die Identität $K = K$ zu einem Turm

$$\begin{array}{l} K \subset K[a_1] \subset K[a_1, a_n] \subset \ldots \subset K[a_1, \ldots, a_n] \\ \| \\ K \subset K[a_1'] \subset K[a_1', a_n'] \subset \ldots \subset K[a_1', \ldots, a_n'] \end{array}$$

von Isomorphismen fortsetzen. Dabei wird a_i auf a_i' abgebildet. Sei $K[a_1, \ldots, a_j] \cong K[a_1', \ldots, a_j']$

schon konstruiert. Dann bildet der auf den Polynomring fortgesetzte Isomorphismus

$$K[a_1,\dots,a_j][x] \cong K[a_1',\dots,a_j'][x]$$

die Faktorisierung

$$f = \prod_{i=1}^{j}(x-a_i)\cdot g \quad \text{auf} \quad f = \prod_{i=1}^{j}(x-a_i')g' \quad \text{ab},$$

also g wird auf g' abgebildet.
Sei $h \in K[a_1,\dots,a_j][x]$ das Minimalpolynom von a_{j+1}. Dann ist h ein Faktor von g.
Es bezeichne h' das Bild von h in $K[a_1',\dots,a_j'][x]$ und sei a_k' eine Nullstelle von h' in $K[a_1',\dots,a_n']$.
Dann gilt a_k' ist Element von $\{a_{j+1}',\dots,a_n'\}$
Nach Umnummerierung können wir $k=j+1$ annehmen
Dann gilt

$$\begin{aligned} K[a_1,\dots,a_j,a_{j+1}] &\cong K[a_1,\dots,a_j][x]/(h) \\ &\cong K[a_1',\dots,a_j'][x]/(h') \\ &\cong K[a_1',\dots,a_j',a_{j+1}'] \end{aligned} \quad \square$$

<u>Bem:</u> 1) Der Isomorphismus

$$K[a_1,\dots,a_n] \to K[a_1',\dots,a_n'] \text{ ist i.A.}$$

nicht eindeutig bestimmt.
Hat das Minimalpolynom von a_1 in $K[a_1',\dots,a_n']$ mehrere Nullstellen, dann können wir für a_1' jede dieser Nullstellen wählen.
2) Sind L und L' Zerfällungskörper von $f \in K[x]$
Dann bildet jeder Isomorphismus $\varphi: L \to L'$ mit $\varphi|_K = id_K$, d. h.

$$\begin{tikzcd} L \arrow[rr, "\varphi"] & & L' \\ & K \arrow[ul, hook] \arrow[ur] & \end{tikzcd}$$

kommutiert
Die Menge der Nullstellen von f bis L bijektiv auf die Menge der Nullstellen f in L' ab.

7.16 Def Sei L Körper. Dann heißt

$$\mathrm{Aut}(L) = \{\varphi : L \to L \mid \varphi \text{ ist ein Automorphismus}\}$$

die Automorphismengruppe von L. Für $K \subset L$ eine Körpererweiterung heißt

$$\mathrm{Aut}[L;K] = \{\varphi : L \to L \mid \varphi \text{ Automorph. von } L \text{ mit } \varphi|_K = \mathrm{id}_K\}$$

die Automorphismengruppe von L über K.

Ist $f \in K[x]$ nicht konstantes Polynom und L ein Zerfällungskörper, dann heißt

$$\mathrm{Gal}(f) = \mathrm{Aut}(L;K]$$

die Galoisgruppe von f über K.

Bem: 1) Sind $a_1, \dots, a_r$ die paarweise verschiedenen Nullstellen von f, dann permutiert jedes $\varphi \in \mathrm{Gal}(f)$ die Nullstellen und die Wirkung von φ auf f ist durch diese Permutation festgelegt.
Eine Durchnummerierung der paarweise verschiedenen Nullstellen $a_1, \dots, a_r$ definiert daher eine Injektion

$$\mathrm{Gal}(f) \hookrightarrow S_r$$

2) Ist f irreduzibel, dann operiert die Galoisgruppe transitiv auf der Menge der Nullstellen, d. h. mit nur einer Bahn. Als Bild von a_1 kommt nämlich jedes andere a_j in Frage da

$$\begin{array}{ccccc} k[a_i] & \xleftarrow{\cong} & k[x]/(f) & \xrightarrow{\cong} & k[a_j] \\ a_i & \leftarrow\!\shortmid & x & \longmapsto & a_j \end{array}$$

Dieser Iso. lässt sich zu einem Automorphismus des Zerfällungskörper fortsetzen.

7.17 Satz Sei $f \in K[x]$ ein Polynom ohne mehrfache Nullstellen in seinem Zerfällungskörper L. Dann gilt

$$|\mathrm{Aut}(L;K)| = [L:K]$$

Beweis Es seien $a_1, \dots, a_n$ die paarweise versch. Nullstellen von f in L, $n = \deg f$, also

$$L = K[a_1, \dots, a_n]$$ ~~dagegen ist~~

Da jedes $\varphi \in \mathrm{Aut}(L;K]$ die Nullstellen als Menge festlässt, ist die Operation durch die Wirkung auf dieser Menge festgelegt.

~~Br~~ Wir betrachten nun den Turm

$$K \subset K[a_1] \subset K[a_1, a_2] \subset \dots \subset K[a_1, \dots, a_n]$$

und fragen welche Wahlmöglichkeiten wir für $\varphi(a_1)$, $\varphi(a_2)$ usw. haben.

Für $\varphi(a_1)$ können wir jede andere Nullstelle a_1' des Minimalpolynoms von a_1 wählen. ~~Also~~ Da f und damit h keine mehrfache Nullstelle hat sind dies genau

$$[K[a_1]:K] \text{ viele Wahlmöglichkeiten.}$$

Nach Wahl der Isomorphie $K[a_1] \cong K[a_1']$ haben wir $\varphi(a_2)$ d.h. für a_2 genau $(K[a_1, a_2] : K[a_1])$ viele Wahlmöglichkeiten, da das Minimalpolynom $h_2 \in K[a_1][x]$ von a_2 auf ein irreduzibles Polynom $h_2' \in K[a_1'][x]$ abgebildet wird, usw.

Insgesamt erhalten wir

$$[K[a_1]:K] \cdot [K[a_1, a_2] : K[a_1]] \dots [K[a_1, \dots, a_n] : K[a_1, \dots, a_{n-1}]]$$
$$= [K[a_1, \dots, a_n] : K]$$

viele Wahlmöglichkeiten. Also

$$|\mathrm{Aut}(L;K)| = [L;K]$$

Bem.: Es kann vorkommen, dass ein irreduzibles Polynom von Grad > 1 nur eine Nullstelle in seinem Zerfällungskörper hat.

<u>Beispiel</u>: Betrachten $K = \mathbb{F}_p(t)$ und das Polynom $f = x^p - t \in K[x]$. f ist irreduzibel

Ist $a \in L$ eine Nullstelle von f, so gilt $a^p = t$ und deshalb $(x-a)^p = x^p - a^p = x^p - t$ da wegen $\mathrm{char}(K) = p$ alle anderen Terme der binom. Formel wegfallen.

$L = K[a]$ und ist der Zerfällungskörper und $\mathrm{Aut}(L;K) = \{id\}$, da für a keine andere Nullstelle gewählt werden kann.

7.18 <u>Satz & Def</u>. Sei K ein Körper der Charakteristik $p > 0$. Dann ist die Abbildung

$$F: K \to K, \quad a \mapsto a^p$$

ein Körperendomorphismus, der sog. Frobeniusendomorphismus.

<u>Beweis</u>: $(ab)^p = a^p b^p$ ist klar

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p$$
$$= a^p + b^p \quad \cancel{\text{da}}$$

, da $p \mid \binom{p}{k}$ für $1 \leq k \leq p-1$ gilt $\square$

F ist natürlich injektiv und wenn K ein endlicher Körper ist auch surjektiv und dann ein ein Körperautom.

Wie stellt man fest, ob ein Polynom eine mehrfache Nullstelle hat? Für $f \in \mathbb{R}[x]$ ist dies der Fall, wenn f und seine Ableitung f' einen gemeinsamen Faktor haben.

Polynome lassen sich formal ableiten:

7.19 <u>Def</u> K Körper und $f \in K[x]$ ein Polynom etwa

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Die Formale Ableitung f' von f definieren wir durch

$$f' = n a_n x^{n-1} + \dots + k a_k x^{k-1} + \dots + a_1$$

7.20 ~~Def~~ Satz Die formale Ableitung

$$': K[x] \to K[x]$$

ist K-linear und genügt der Produktregel

$$(fg)' = f'\cdot g + fg'$$

Es gilt weiter $((x-a)^n)' = n(x-a)^{n-1}$

<u>Beweis</u>: Die K-linearität ist klar. Es reicht daher die Produktregel für Monome zu zeigen.

$$\begin{aligned}(x^n \cdot x^m)' = (x^{n+m})' &= (n+m)x^{n+m-1} \\ &= nx^{n-1}\cdot x^m + mx^n \cdot x^{m-1} \\ &= (x^n)'x^m + x^n(x^m)'\end{aligned}$$

Die letzte Formel zeigen wir per Induktion nach n.

$$(x-a)' = 1 = (x-a)^0$$

$$\begin{aligned}((x-a)^n)' = ((x-a)^{n-1}(x-a))' &\underset{\substack{\text{Prod.}\\ \text{regel}\\ \text{IV}}}{=} (n-1)(x-a)^{n-2}(x-a) + (x-a)^{n-1}\cdot 1 \\ &= n(x-a)^{n-1} \qquad \square\end{aligned}$$

7.21 <u>Satz</u> 1) $K \subset L$ Körpererweiterung

Dann stimmt die Ableitung f' von $f \in K[x]$ mit der von f in $L[x]$ überein.

2) Für Körper K mit $\operatorname{char}(K) = 0$ gilt

$$f' \equiv 0 \iff f \text{ ist konstant}$$

Für K mit $\operatorname{char}(K) = p > 0$ gilt

$$f' \equiv 0 \iff f \in K[x^p] \subset K[x].$$

3) f hat eine mehrfache Nullstelle in seinem Zerfällungskörper $\iff \operatorname{ggT}(f, f')$ hat Grad ≥ 1.

Beweis

1) klar. f' ist durch die Regel

$$(x^n)' = nx^{n-1}$$

2) $(x^n)' = nx^{n-1} \neq 0$ für $n>0$ und $char(K)=0$ oder n mit $p \nmid n$ für $char(K)=p$

$char(K)=p$, und x^{kp} haben wir

$$(x^{kp})' = kpx^{kp-1} = 0, \text{ da } p \cdot 1 = 0 \in K$$

Also $char(K)=p$ gilt $f'=0 \iff f \in K[x^p] \subset K[x]$

3) Sei $f = \lambda \cdot \prod_{k=1} (x-a_k)^{v_k}$

die Faktorisierung von f in seinen Zerfällungskörper.

Wir schreiben $f = (x-a_k)^{v_k} \cdot g$ mit $g(a_k) \neq 0$

$\Rightarrow f' = v_k (x-a_k)^{v_k - 1} g + (x-a_k)^{v_k} g'$

Für $v_k \geq 2$ folgt $(x-a_k)^{v_k-1}$ f und f' teilt, also

$(x-a_k) \mid ggT(f, f')$ und $\deg ggT(f, f') \geq 1$

ist $v_k = 1$ also

$f = (x-a_k) g$ ~~so~~ haben wir $f' = g + (x-a_k) \cdot g'$ und wegen

$g(a_k) \neq 0$ ist

$(x-a_k)$ kein Teiler von f.

Sind also alle $v_k = 1$ dann haben f und f' keinen gemeinsamen Faktor. $\square$

7.22 Satz (Klassifikation von endlichen Körper)

Zu jeder Primzahlpotenz $q = p^r$ gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit q Elementen, nämlich den Zerfällungskörper von $f = x^q - x \in \mathbb{F}_p[x]$

Die Galoisgruppe $Aut(\mathbb{F}_q, \mathbb{F}_p)$ ist zyklisch von der Ordnung r und wird von Frobeniusautomorphismen $F: \mathbb{F}_q \to \mathbb{F}_q$, $a \mapsto a^p$ erzeugt. Die Multiplikative Gruppe $\mathbb{F}_q^\times$ ist zyklisch von der Ordnung $q-1$.

__Beweis Existenz__ Wir betrachten den Zerfällungskörper von

$f = x^q - x \in \mathbb{F}_p[x]$

Da $f' = qx^{q-1} - 1 = -1$ gilt $ggT(f, f') = 1$

f hat also keine mehrfache Nullstellen und damit genau q Nullstellen. Um einzusehen, dass $\mathbb{F}$ mit der Menge dieser Nullstellen übereinstimmt, betrachten wir die r-te Potenz des Frobeniusautomorphismus

$$F^r : \mathbb{F} \to \mathbb{F}, \quad a \mapsto ((a^p)^{p \cdots}) \cancel{(a^{p^r})} = a^q$$

Da $(a+b)^q = q a^q + b^q$ gilt, ist mit a, b Nullstelle von f aber $a^q = a$, $b^q = b$ auch $a+b$ eine Nullstelle.

$(a \pm b)^q = a^q \pm b^q = a \pm b$

Die ~~Summen~~ Nullstellen $f = x^q - x$ bilden also einen Unterkörper von $\mathbb{F}$, der mit $\mathbb{F}$ übereinstimmt, da der Zerfällungskörper der kleinste Körper ist, über dem f in Linearfaktoren zerfällt.

__Eindeutigkeit__ Sei $\mathbb{F}$ ein beliebiger endlicher Körper $p = char(\mathbb{F})$ und $r = [\mathbb{F} : \mathbb{F}_p]$. Dann hat $\mathbb{F}$ $q = p^r$ Elemente, da $\mathbb{F} \supset \mathbb{F}_p{}^r$ als $\mathbb{F}_p$-Vektorraum.

Die Multiplikative Gruppe $(\mathbb{F}^\times, \cdot)$ hat Ordnung $q-1$. Die Ordnung jedes Elements $a \in \mathbb{F}^\times$ ist ein Teiler von $q-1$ und deshalb $a^{q-1} = 1 \; \forall a \in \mathbb{F}^\times$.

Jedes Element $\mathbb{F}^\times$ ist also eine Nullstelle von

$$x^{q-1} - 1$$

und $x^q - x = x \cdot (x^{q-1} - 1)$ hat alle Elemente von $\mathbb{F}$ als Nullstelle. Die multiplikative Gruppe $(\mathbb{F}^\times, \cdot)$ ist zyklisch. ~~Andernfalls~~ Nach dem Elementarteilersatz ist

$$(\mathbb{F}^\times, \cdot) \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_r$$

wobei $1 < d_1 | d_2 | \ldots | d_r$ und $q - 1 = d_1 \cdot \ldots \cdot d_r$

Wäre $r>1$, dann hätten wir $d_r < q-1$ und jedes Element von $(\mathbb{F}^\times, \cdot)$ wäre eine Nullstelle von $X^{d_r}-1$.
Dieses Polynom hat aber höchstens d_r Nullstellen
Also $r=1$, $d_r=q-1$, $(\mathbb{F}^\times,\cdot) \cong \mathbb{Z}/(q-1)$ ist zyklisch.
$F: \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$ ist ein Element von $(\mathrm{Aut}(\mathbb{F}, \mathbb{F}_p))$.
Ist $a \in \mathbb{F}^\times$ ein Erzeuger von $(\mathbb{F}^\times, \cdot)$, dann gilt $a^d \neq 1 \ \forall d < q-1$
Also

$$F^s(a) = a^{p^s} \neq a \ \forall s < r, \text{ da } p^s - 1 < q-1 = p^r - 1$$

$$F^r = \mathrm{id}_{\mathbb{F}_q}, \text{ da } a^q = a \ \forall a \in \mathbb{F} = \mathbb{F}_q \text{ gilt.}$$

Also

$$\begin{array}{c} \langle F \rangle \cong \mathbb{Z}/r \\ \cap \\ \mathrm{Aut}(\mathbb{F}_q ; \mathbb{F}_p) \end{array}$$

da wir für Zerfällungskörper $L \supset K$ eines Polynoms ohne mehrfache Nullstellen:

$$[L:K] = |\mathrm{Aut}(L;K)|$$

kann es keine weiteren Automorphismen geben. Also

$$\mathrm{Aut}(\mathbb{F}_q ; \mathbb{F}_p) = \langle F \rangle \cong \mathbb{Z}/r \qquad \square$$

§8 Galois Theorie

Evariste Galois (25.10.1811 – 31.5.1832)

8.1 Definition

Sei L ein Körper und $G \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann heißt

$$\mathrm{Fix}(G) = \{a \in L \mid \varphi(a) = a \ \forall \varphi \in G\}$$ der

Fixkörper von G.

Dies ist ~~ein~~ Körper, da mit $a, b \in \mathrm{Fix}(G)$

$$\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = a \pm b$$

Eine Körpererweiterung $K \subset L$ heißt galoissch wenn es eine endliche Untergruppe $G \subset \mathrm{Aut}(L)$ gibt mit $\mathrm{Fix}(G) = K$. Dann ist $G \subset \mathrm{Aut}(L;K) \subset \mathrm{Aut}(L)$

Bem Man kann die Vorraussetzung, dass G eine endliche Untergruppe ist, fallen lassen.
Dies gibt eine kompliziertere Theorie in der auch gewisse Topologische Konzepte eine Rolle spielen (s. Bosch)
$Aut(\overline{\mathbb{Q}})$ ist unverstanden

8.2 Satz Sei $K \subset L$ eine Galoiserweiterung mit Galoisgruppe G. Dann gilt

$$|G| = |Aut(L;K)|$$

Mit anderen Worten $G \subset Aut(L)$ endlich dann gilt

$$[L; Fix(G)] = |G|$$

Beispiele: 1) Sei f ein Polynom $\in K[x]$ ohne mehrfache Nullstellen. L sei Zerfällungskörper. Wir haben schon gezeigt $[L:K] = |Aut(L;K)|$
Noch nicht so klar für $G = Aut(L;K)$ ist

$$K = Fix(G)$$

$K \subset Fix(G)$. Mit obigen Satz

$$[L:K] = |G| = \underset{\overset{\shortparallel}{G}}{[L: Fix(G)]} \cdot \underbrace{[Fix(G):K]}_{=1} \text{ folgt}$$

$K = Fix(G)$
$L \supset K$ eine Galoiserweiterung.

2) $\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$ ist keine Galoiserweiterung.
Das Minimalpolynom von $\sqrt[3]{2}$ ist x^3-2 und diese Funktion hat nur eine Nullstelle in $\mathbb{R}$
$\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$ und daher
$Aut(\mathbb{Q}[\sqrt[3]{2}]\mathbb{Q}) = \{id\}$

3) $\mathbb{F}_q \supset \mathbb{F}_p$ ist eine Galoiserweiterung mit Galoisgruppe $\langle F \rangle \cong \mathbb{Z}/r$.

Der Beweis von 8.2 nach Artin verwendet Charaktere

8.3 Def Sei G eine Gruppe und L ein Körper.
Ein Charakter von G mit Werten in L ist ein Gruppenhomomorphismus $\chi : G \to (L^\times, \cdot)$

8.4 Lemma (E. Artin)
Paarweise verschiedene Charaktere
$\chi_1, \dots, \chi_n$ von einer Gruppe G mit weiter L
sind linear unabhängig in dem L-Vektorraum
$(\mathrm{Abb}(G, L))$ aller Abbildungen von G nach L.

Beweis: Induktion nach n.
$\lambda \chi_1 = 0 \quad \Rightarrow \lambda \chi_1(e) = \lambda \cdot 1 = \lambda$.
Sei nun die Aussage für $n-1$-Charaktere schon gezeigt und $\chi_1, \dots, \chi_n$ paarweise verschieden, $n \geq 2$.
Dann existiert ein $a \in G$, sodass
$\chi_1(a) \neq \chi_n(a)$
Sei $0 = \lambda_1 \chi_1 + \dots + \lambda_n \chi_n$
Einsetzen von $a \cdot g$ gibt
$0 = \lambda_1 \chi_1(a) \cdot \chi_1(g) + \dots + \lambda_n \chi_n(a) \cdot \chi_n(g)$
g einsetzen und mit $\chi_n(a)$ multiplizieren liefert
$0 = \lambda_1 \chi_n(a) \chi_1(g) + \dots + \lambda_n \chi_n(a) \cdot \chi_n(g)$
Die Differenzierbarkeit
$\forall g \in G \quad 0 = \lambda_1 (\chi_1(a) - \chi_n(a)) \chi_1(g) + \dots + \lambda_{n-1}(\chi_{n-1}(a) - \chi_n(a)) \cdot \chi_{n-1}(g)$
$\Rightarrow 0 = \lambda_1 (\chi_1(a) - \chi_n(a)) \chi_1 + \dots + \lambda_{n-1} (\chi_{n-1}(a) - \chi_n(a)) \chi_{n-1}$
Induktionsvorr $\Rightarrow \lambda_1 (\chi_1(a) - \chi_n(a)) = 0 \Rightarrow \lambda_1 = 0$
Nochmals die Induktionsvorraussetzung liefert
$\lambda_2 = \dots = \lambda_n = 0$

8.5 Korollar Sind $\varphi_1, \dots, \varphi_n$ paarweise verschiedene Monomorphismen $L \to M$ zwischen Körpern. Dann $\varphi_1, \dots, \varphi_n$ linear unabhängig in dem M-Vektorraum $\mathrm{Abb}(L, M)$

Beweis: $\chi_k = \varphi_k|_{L^\times} : L^\times \to M^\times$ sind Charaktere und da $\varphi_k(0) = 0$ sind $\varphi_1, \dots, \varphi_n$ paarweise verschieden

$$\Leftrightarrow \chi_1, \dots, \chi_n \quad \text{"} \quad \text{"}$$

Also $\varphi_1, \dots, \varphi_n$ sind linear unabhängig.

8.6 Satz Es seien $\varphi_1, \dots, \varphi_n$ paarweise verschiedene Monomorphismen $L \to M$ zwischen zwei Körpern. Dann ist

$$K = \{a \in L \mid \varphi_1(a) = \dots = \varphi_n(a)\}$$

ein Unterkörper von L mit

$$[L:K] \geq n$$

Beweis: Dass K ein Unterkörper ist, gilt da die φ_k Homomorphismen sind.

Angenommen $[L:K] = r < n$ und $a_1, \dots, a_r \in L$ eine Basis als K-Vektorraum.

Dann hat das lineare Gleichungssystem

$$\begin{aligned} \varphi_1(a_1)x_1 + \dots + \varphi_n(a_1)x_n &= 0 \\ &\vdots \\ \varphi_1(a_r)x_1 + \dots + \varphi_n(a_r)x_n &= 0 \end{aligned}$$

eine nicht triviale Lösung $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in M^n$

Da es zu jedem $a \in L$, $\lambda_1, \dots, \lambda_r \in K$ gibt mit $a = \lambda_1 a_1 + \dots + \lambda_r a_r$ und $\varphi_i(\lambda_j) = \varphi_1(\lambda_j)$

$$\Rightarrow \sum_{i=1}^{n} \varphi_i(a) y_i = \sum_{i=1}^{n} \sum_{j=1}^{r} \varphi_i(\lambda_j) \varphi_i(a_j) y_i$$

$$= \sum_{j=1}^{r} \varphi_1(\lambda_j) \cdot \underbrace{\sum_{i=1}^{n} \varphi_i(a_j) y_i}_{=0}$$

Also $\sum_{i=1}^{n} \varphi_i y_i$ ist die Nullabbildung

Dies widerspricht dem Lemma

Damit ist $[L : \mathrm{Fix}(G)] \geq |G|$ gezeigt.