Übungsblatt 7

Aufgabe 1

(1) Bmk: p Primzahl, dann $p \mid \binom{p}{k}$ $\forall\, k = 1, \dots, p-1$

$\binom{p}{k}$ ↑ Binomialkoeffizient $\in \mathbb{Z}$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow p \mid p! = \binom{p}{k} \underbrace{k!(p-k)!}_{\text{teilerfremd mit } p,\ \text{da } 1<k<p} \Rightarrow p \mid \binom{p}{k}$$

$\varphi(0) = 0$; $\varphi(1) = 1$, $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\cdot\varphi(b)$

$$\varphi(a+b) = (a+b)^p \underset{\text{↑ Binomformel}}{=} a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p \underset{\text{Bmk}}{=} a^p + b^p =$$

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

(2) $R = \mathbb{F}_p[t]$ faktoriell

$X^p - t \in R[X]$ ist irreduzibel nach (Satz von Eisenstein für das Primelement $t \in R$)

$X^p - t$ normiert $\Longrightarrow$ (Satz von Gauß) irreduzibel in $Q(R)[X] = K[X]$.

Sei α eine Nullstelle von $X^p - t$ in $\overline{K}$

Dann gilt $\alpha^p = t$ in $\overline{K}$ und $X^p - t = X^p - \alpha^p = (X-\alpha)^p$ in $\overline{K}[X]$

$\Rightarrow$ $X^p - t$ ist nicht separabel

Aufgabe 2 Angenommen, $X^p - a$ ist reduzibel in $K[X]$

~~Sei~~ Q ~~ein irreduzibler Teiler von $X^p - a$~~

mit einem irreduziblen Teiler $Q \in K[X]$, $1 \leq m = \text{Grad } Q < p$

Multiplikation mit X: $\varphi : \frac{K[X]}{Q} \longrightarrow \frac{K[X]}{Q}$

als K-lineare Abbildung $v \longmapsto X \cdot v$

$$\dim_K \frac{K[X]}{Q} = \text{Grad } Q = m.$$

$\varphi^2 = \varphi \circ \varphi \quad v \longmapsto X^2 \cdot v$

$\vdots$

$\varphi^p : v \longmapsto X^p \cdot v = a v$

~~$\varphi^2 = \varphi \circ \varphi =$~~

$$\varphi^p = a \cdot id_m \quad \left(\leftarrow \text{Einheitsmatrix } a \cdot E_m \right)$$

$$\det \varphi^p = \det (a \cdot id)$$

$$(\det \varphi)^p = a^{\dim \frac{K[X]}{Q}} = a^m$$

$a < m < p \Rightarrow g.g.T(m,p) = 1 \Rightarrow \exists\, l \in \mathbb{Z}$ mit $ml \equiv 1 \mod p$

(Bezout Lemma)

Dann $(\det \varphi)^{pl} = a^{ml} = a^{1+p \cdot k} = a \cdot a^{pk}$

$$\Rightarrow a = \frac{(\det \varphi)^{pl}}{a^{pk}} = \left(\frac{\det \varphi^l}{a^k} \right)^p$$

Widerspruch mit $a \notin K^{*p}$

Aufgabe 3

(1)

$1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$ sind verschiede komplexe NS von $X^p - 1$

$\left((\zeta_p^k)^p = (\zeta_p^p)^k = 1^k = 1 \right)$

Dann $\sqrt[p]{a}, \sqrt[p]{a}\,\zeta_p, \dots, \sqrt[p]{a}\,\zeta_p^{p-1}$ sind die NS von $X^p - a$ in $\mathbb{C}$

Es folgt: $L = \mathbb{Q}(\sqrt[p]{a}, \sqrt[p]{a}\,\zeta_p, \dots, \sqrt[p]{a}\,\zeta_p^{p-1}) = \mathbb{Q}(\sqrt[p]{a}, \zeta_p)$

(2)

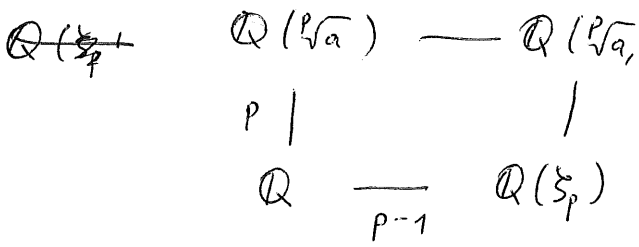
Nach Aufgabe 2 ist $X^p - a$ irreduzibel in $\mathbb{Q}[X]$

$\Rightarrow$ $X^p - a$ ist das Minimalpolynom von $\sqrt[p]{a}$ über $\mathbb{Q}$

$\Rightarrow$ $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$

ζ_p ist eine NS von $\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + 1$ und dieses Polynom ist irr. in $\mathbb{Q}[X]$

Es folgt: $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$



$\Rightarrow$ $X^p - a$ bleibt irreduzibel über $\mathbb{Q}(\zeta_p)$

$\Downarrow$

$[\mathbb{Q}(\sqrt[p]{a}, \zeta_p) : \mathbb{Q}(\zeta_p)] = p$

$\Downarrow$ Gradformel

$[L : \mathbb{Q}] = p(p-1)$

Aufgabe 4

$f(x) = g(X^{p^r})$

$g \in K[X]$ ist irreduzibel (sonst $g = P \cdot Q$ und $f(x) = g(x^{p^r}) = P(x^{p^r}) \cdot Q(x^{p^r})$ reduzibel)

r maximal $\Rightarrow$ $g \neq h(x^p)$ mit $h \in K[X]$

(sonst $f = g(x^{p^r}) = h(x^{p^{r+1}})$ $\lightning$ mit Maximalität von r)

$\Longrightarrow$ $g'(x) \neq 0$ $\Rightarrow$ g ist separabel

Bmk, Seite 50

Lemma 3.26 b

Sei $g = (x-\beta_1) \cdot \ldots \cdot (x-\beta_k)$ in $\overline{K}[X]$ (alle $\beta_i \in \overline{K}$ sind verschiedene)

Dann $f(x) = g(x^{p^r}) = (x^{p^r}-\beta_1) \cdot \ldots \cdot (x^{p^r}-\beta_k) =$

$= (x^{p^r}-\alpha_1^{p^r}) \cdot \ldots \cdot (x^{p^r}-\alpha_k^{p^r}) = (x-\alpha_1)^{p^r} \cdot \ldots \cdot (x-\alpha_k)^{p^r}$,

wobei α_i ist eine Nullstelle von $X^{p^r}-\beta_i$ in $\overline{K}$.

Aufgabe 5

G Gruppe, X Menge

G wirkt auf X $\Leftrightarrow$ $\exists\, \varphi : G \times M \longrightarrow M$
$(g, m) \longmapsto g.m$
mit folgenden Eigenschaften:

1) $e.m = m \quad \forall\, m \in M$

2) $g'.(g.m) = (g'g).m$
$\forall\, g, g' \in G$ und $m \in M$

Sei $G \to M,\ g \to \varphi(g,m) = g.m$ injektiv $\forall\, m \in M$.

Dann $gm = m \Leftrightarrow \varphi(g,m) = \varphi(e,m) \Longrightarrow g = e$
da $G \to M$, $g \mapsto g.m$ injektiv.

Angenommen, die Wirkung frei ist.

und $\varphi(g_1, m) = \varphi(g_2, m) \Leftrightarrow g_1.m = g_2.m \Leftrightarrow$

$\Leftrightarrow g_1^{-1}.(g_1.m) = g_1^{-1}.(g_2.m) = (g_1^{-1}g_2).m$ $\overset{\text{Wirkung ist frei}}{\Rightarrow} g_1^{-1}g_2 = e \Rightarrow$

$\Rightarrow g_1 = g_2$

$g_1^{-1}.(g_1.m) \overset{2)}{=} e.m = m$

Es folgt:
$G \to M,\ g \mapsto \varphi(g,m)$
ist injektiv $\forall\, m \in M$

$\forall\, m \in M$
$g \longmapsto \varphi(g,m)$ ist surjektiv

$\Updownarrow$

$\forall\, m, m' \in M$, $\exists\, g \in G$ mit $m' = \varphi(g,m) = g.m$

$\Updownarrow$

die Wirkung ist transitiv.

Aufgabe 5

Seien L/K normale Körpererweiterung, $\sigma \in \mathrm{Hom}_K(L, \bar{K})$ und $\varphi \in \mathrm{Aut}_K(L)$

- $\sigma \circ \varphi^{-1} = \sigma \Longrightarrow \varphi^{-1} = id_L \Rightarrow \varphi = id \Rightarrow$ die Wirkung ist frei
  (σ injektiv)

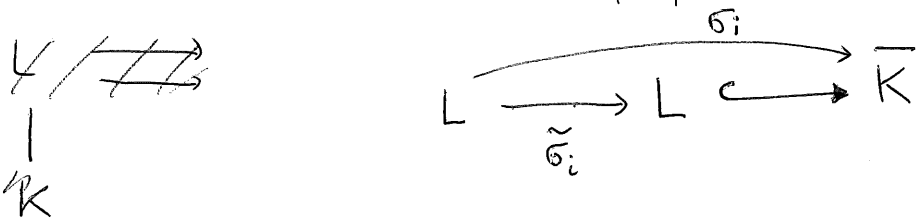
- Seien $\sigma_1, \sigma_2 \in \mathrm{Hom}_K(L, \bar{K})$. z.z.: $\exists\, \varphi \in \mathrm{Aut}_K(L)$ mit $\sigma_1 = \sigma_2 \circ \varphi^{-1}$

L = Zerfällungskörper von $\{f_i\}_{i \in I}$, $f_i \in K[X]$.

σ_i (eine NS von f_i) = eine NS von f_i

$\sigma_1(L) = \sigma_2(L) = L \subset \bar{K}$

Dann σ_i ist die Komposition



Dann $\sigma_1 = \sigma_2 \circ \underbrace{\tilde{\sigma}_2^{-1} \circ \sigma_1}_{\in \mathrm{Aut}_K(L)}$

Für $\varphi^{-1} = \tilde{\sigma}_2^{-1} \circ \sigma_1$, $\varphi = \tilde{\sigma}_1^{-1} \circ \sigma_2$ gilt $\sigma_1 = \sigma_2 \circ \varphi^{-1} = \varphi \cdot \sigma_2$