Weiter zu A21: Endliche Körper

$\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p \rightsquigarrow \mathbb{F}_{p^e} \mid \mathbb{F}_p$

21.5. Satz (Bestimmung aller endlichen Körper):

(1) $\forall p$ prim $\forall n \geq 1$ $\exists$ bis auf Iso genau ein endl. Körper $\mathbb{F}_{p^n}$, $\#\mathbb{F}_{p^n} = p^n$, nämlich: $\mathbb{F}_{p^n} := \mathbb{Z}K$ von $f = \underbrace{T^{p^n} - T}_{\text{(sep.)}} \in \mathbb{F}_p[T]$.

(2) $a \in \mathbb{F}_{p^n} \iff f(a) = 0$.

(3) K endl. Körper $\Rightarrow \exists p$ prim $\exists n \geq 1 : K \cong \mathbb{F}_{p^n}$.

Bew.: (1): Ex: Sei $p \in \mathbb{N}$ prim, $n \geq 1$. Sei $\mathbb{F}_p[T] \ni f(T) = T^{p^n} - T$.

$(-1 = p-1)$

f ist separabel, da $f' = \underbrace{p^n}_{=0} T^{p^n-1} - 1 = -1$ teilerfremd zu f.

$\mathbb{F}_{p^n} \overset{!}{=} X$

$\mathbb{F}_p$

Sei K der $\mathbb{Z}K$ von f über $\mathbb{F}_p$ und

Sei $X := \{x \in K;\ f(x) = 0\}$, $\#X = p^n$, da f separabel.

Sei σ der Frobenius-Endo von K,

d.h. $\sigma : K \to K$, $x \mapsto x^p$ (inj.).

Somit: $X = \{x \in K;\ \sigma^n(x) = \underbrace{x^{p^n} = x}_{f(x)=0}\} =: \mathrm{Fix}(\sigma^n)$.

Für jeden Körperendo τ ist $\mathrm{Fix}(\tau) := \{x \in K;\ \tau(x) = x\}$ ein Körper, der in K liegt,

also $X = K$ (da X $\mathbb{Z}K$ von f über $\mathbb{F}_p$).

Da f separabel, ist $\#K = p^n$. Bezeichnung: $\mathbb{F}_{p^n} := K$.

Eind.: Sei K nun ein endl. Körper, $\#K = p^n$.

Es ist $\#K^\times = p^n - 1$, d.h. $\forall x \in K^\times : \underbrace{x^{p^n-1} = 1}$. ✓

↑ da $\mathrm{ord}(x) \mid \#K^\times = p^n - 1$ (↳ $= \min\{\ell : x^\ell = 1\}$ Lagrange)

[Vgl.: $K^\times \overset{=\langle a \rangle}{=}$ zyklisch nach Satz 21.2 ↳ $\forall x \in K^\times : x = a^e \to x^{p^n-1} = (a^e)^{p^n-1} = (\underbrace{a^{p^n-1}}_{=1})^e = 1$]

$\Rightarrow$ Jedes $x \in K$ ist Wurzel von $T^{p^n} - T = T \cdot (T^{p^n - 1} - 1) \in \mathbb{F}_p[T]$,
d.h. K ist ZK von $T^{p^n} - T \in \mathbb{F}_p[T]$ über $\mathbb{F}_p$, also eind. Erw.

(2): $a \in \mathbb{F}_{p^n} \Leftrightarrow a \in X = \{x \in \mathbb{F}_{p^n} ; f(x) = 0\} \Leftrightarrow f(a) = 0$.

(3): Sei K endl. Körper, $p := \mathrm{Char}(K)$, d.h.
PrimKörper $\mathrm{Prim}(K) \cong \mathbb{F}_p$, sei also $\mathbb{F}_p \subseteq K$.
Da K ein $\mathbb{F}_p$-VR, sei $x_1, \dots, x_n \in K$ eine $\mathbb{F}_p$-Basis von K, dann:

$$K \overset{\text{VR-Iso}}{\cong} \underbrace{\mathbb{F}_p \oplus \dots \oplus \mathbb{F}_p}_{n\text{-mal}} \cong (\mathbb{F}_p)^n = \mathbb{F}_p^n,$$

d.h. $\#K = p^n$. Nach (1): $K \cong \mathbb{F}_{p^n}$. $\square$

Bsp.: $\mathbb{F}_4 = $ ZK von $T^4 - T = T(T^3 - 1) = T(T-1) \cdot (T^2 + T + 1)$.
Charakteristik 2: $2 = 1 + 1 = 0 \Leftrightarrow 1 = -1$ $\qquad (T-a)\cdot(T-b)$

$\mathbb{F}_4 = \{0, 1, a, b\} \supseteq \mathbb{F}_2 = \{0, 1\}$

$(T-a)(T-b) = T^2 + T + 1$
$T^2 - (a+b)T + ab \rightsquigarrow ab = 1$, $a + b = 1$
$+b \Rightarrow a + \underbrace{b + b}_{=0} = 1 + b$

$(T^3 - 1) : (T-1) = T^2 + T + 1$
$-(T^3 - T^2)$
$T^2 - 1$
$-(T^2 - T)$
$T - 1$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

$a^2 + a + 1 = 0$
$a^2 = a + 1 = b$

$T^2 + T + 1 = 0 \rightsquigarrow T_{1/2} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} - 1} = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3} \in \mathbb{C}$

$\rightsquigarrow a = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$, $b = -\frac{1}{2} - \frac{i}{2}\sqrt{3}$

Informatik:
$\mathbb{F}_{2^8} =$ "AES-Körper"

$\rightsquigarrow \mathbb{F}_4 = \mathbb{F}_2[a, b] = \mathbb{F}_2\left[-\frac{1}{2} + \frac{i}{2}\sqrt{3}, -\frac{1}{2} - \frac{i}{2}\sqrt{3}\right]$
$\rightsquigarrow \in \mathbb{C}$

21.6. **Satz**: $\forall$ endl. Körper K $\forall m \geq 1$ $\exists$ (bis auf Iso über K genau ein) L/K: $[L:K] = m$. Dann: L normal, separabel, einfach (vgl. A20.16 vom prim. El.).
Also: K perfekt.

Bew.: Geg. K, $m \geq 1$. Sei $q := \#K = p^n$, $L' := \mathbb{F}_{p^{nm}} = \mathbb{F}_{q^m}$.

L — $L' = \mathbb{F}_{p^{nm}}$
$K = \mathbb{F}_{p^n}$
$\mathbb{F}_p$

Dann: $\#(L'^\times) = q^m - 1 = (q-1)\cdot(q^{m-1} + \dots + q + 1)$,
laut Satz 21.2 ist $L'^\times$ zyklisch.
Somit enthält $L'^\times$ eine UG der Ordnung $q-1$
$\ulcorner L'^\times = \langle a \rangle \rightsquigarrow a^{q^m - 1} = 1$
$b := a^{q^{m-1} + \dots + q + 1} \rightsquigarrow b^{q-1} = a^{q^m - 1} = 1$
b hat Ordn. $q-1 \rightsquigarrow \#\langle b \rangle = q-1$ ↯.

$\Rightarrow L'$ enthält zK K' von $T^q - T \in \mathbb{F}_p[T]$ über $\mathbb{F}_p$,
also $K' = \mathbb{F}_{p^n} \cong K$. Sei $\subseteq K \subseteq L'$

* Ein., normal, sep.:
Jede Erw. L/K, $[L:K] = m$ hat Grad n über $\mathbb{F}_p$,
ist also zK des sep. $T^{p^{nm}} - T \in \mathbb{F}_p[T]$.
Also: L ein., normal, separabel über $\mathbb{F}_p$ bzw. über K.

* Sei x ein erzeugendes El. der Gruppe $L^\times$ (zyklisch nach 21.3),
also $L = K(x)$. □

K — K } endliche Körpererw. sind leicht zu verstehen!
$\mathbb{Q}$ — $\mathbb{F}_p$ }

Haben: $\operatorname{char} K = 0 \Rightarrow$ sep.
$\operatorname{char} K = p$ und K endl. $\Rightarrow$ sep.
Also: in sep. Körpererw. ex. nur als unendl. Körper über $\mathbb{F}_p$, z.B.
$\operatorname{Quot}(\mathbb{F}_p[T]) = \mathbb{F}_p(T)$.

Teil IV: Galoistheorie: Körpertheorie ⇝ Gruppentheorie
↳ E. Galois: ILIAS → "Vorl. Algebra"

A22: Galoisgruppen

Körpererw.

22.1. Einl.: Def. $Gal(L|K)$ Galoisgruppe → Gruppentheorie
sep. & norm. → galois

22.2. Def.: Sei $L|K$. Galoisgruppe von $L|K$
$Gal(L|K) := \{\sigma$ Automorphismus von $L|K$, $\sigma_{|K} = id_K\}$

22.3. Def.: Endl. Erw. $L|K$ galois $:\Leftrightarrow$ $L|K$ normal und separabel

22.4. Satz: $L|K$ galois ↳ "Galois-Erweiterung"
$\Rightarrow \#Gal(L|K) = [L:K]$.

Bew.: $L \to L$ über K sind K-linear.
sep. \ / norm.
K
Einbettungen: $\sigma: L \to L$ (= inj. Körperhom.)
$\sigma(ax) = \underbrace{\sigma(a)}_{=a}\sigma(x) = a\sigma(x)$

also: inj. $\Leftrightarrow$ surj. $\Leftrightarrow$ σ Auto.

$\#Gal(L|K) = \#\Sigma = [L:K]$ (Lemma A20.11) □

22.5. Bsp.: Sei $Char K \neq 2$, $a \in K$ kein Quadrat [d.h. $\nexists b \in K: a = b^2$].
Dann $T^2 - a \in K[T]$ irred. über K.
Sei x Wurzel in einer geeigneten Erw. von K.
$\Rightarrow K(x)|K$ sep., da $2T$ ($\neq 0$ da $char K \neq 2$), T^2-a teilerfremd,
und normal, da $f := T^2 - a = (T-x)(T+x)$ ($-x \neq +x$ da $char K \neq 2$)
Daher: $K(x)|K$ galois. ⇝ Dann: $G := Gal(K(x)|K)$, $\#G = [K(x):K] = 2$
$\Rightarrow G$ zyklisch: $G = \langle\sigma\rangle$ [$\sigma \neq id_K \Rightarrow \sigma(\underbrace{a+bx}_{\in K(x)}) = a + b\underbrace{\sigma(x)}_{-x} = a - bx$]
$= \{id_K, \sigma\}$ ⌟

22.6. **Bsp.:** Betr. $\mathbb{Q}(\sqrt[p]{2})$, $p \in \mathbb{N}$ prim, $p \geq 3$.
$T^p - 2 \in \mathbb{Q}[T]$ Mipo von $\sqrt[p]{2}$.
$\mathbb{Q}(\sqrt[p]{2})$ ist nicht normal, s. Bsp. A19.9 $\rightsquigarrow \mathbb{Q}(\sqrt[p]{2}, e^{2\pi i/p})$ wäre normal.
Also: nicht galois $/\mathbb{Q}$.

22.7. **Bsp.:** Betr. $\mathbb{Q}(\sqrt{2},\sqrt{3}) / \mathbb{Q}$, ist sep. und normal (Zk von $(T^2-2)\cdot(T^2-3)$), also galois. Ferner: $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

$K := \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\mathbb{Q}(\sqrt{2})$ (2) / (2) $\mathbb{Q}(\sqrt{3})$

(2) $\mathbb{Q}$ (2)

Betr. Gruppenhom.: ($\cong C_2$, $\cong C_2$)

$\tau: \mathrm{Gal}(K|\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})|\mathbb{Q})$

$\sigma \mapsto (\sigma_{|\mathbb{Q}(\sqrt{2})}, \sigma_{|\mathbb{Q}(\sqrt{3})})$

Haben:

$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) \cong C_2 \times C_2$,

nach Bsp. 22.5.

τ ist inj.: $\sigma_{|\mathbb{Q}(\sqrt{2})} = id_{\mathbb{Q}(\sqrt{2})} \Rightarrow \sigma(\sqrt{2}) = \sqrt{2}$
$\sigma_{|\mathbb{Q}(\sqrt{3})} = id_{\mathbb{Q}(\sqrt{3})} \Rightarrow \sigma(\sqrt{3}) = \sqrt{3}$
$\Rightarrow \sigma = id_K$

<1 2.7. $\ker\tau = \{id\}$

Also: τ Gruppeniso!

Somit: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})) \cong C_2 \times C_2$.

22.8. **Bem.:** Ex. $L/\mathbb{Q}$ mit $\mathrm{Gal}(L|\mathbb{Q}) \cong G$ vorgegeben ? Ungelöst!