galois = $\overset{A19}{\text{normal}}$ & $\overset{A20}{\text{separabel}}$

Noch zu A20:

$f \in K[T]$ separabel $:\Leftrightarrow$ f hat in einem ZK L lauter versch. Wurzeln,
d.h. $f = a\prod_{i=1}^{n}(T - x_i)$, die $x_i \in L$ pwv.

In Char $K = 0$: Jedes $f \in K[T]$, das irred. ist, ist separabel. (A20.8)

20.9. Def.: Sei $L|K$, $x \in L$ sei alg. $|K$.
x heißt separabel über K $:\Leftrightarrow$ $\exists$ sep. $f \in K[T]$: $f(x) = 0$
$\Leftrightarrow$ Mipo von $x|K$ ist sep.

20.10. $L|K$ heißt separable (alg.) Körpererweiterung von K
$:\Leftrightarrow \forall x \in L$: x ist sep. $|K$

$$\begin{array}{c} L \\ | \\ K \end{array}$$

Gegenteil: inseparabel

20.11. Lemma: Sei $\sigma: K \to K'$ Iso, $L = K(x_1, \dots, x_n)$ alg. $|K$, $E'|K'$ endl. Erw.
Sei $\Sigma := \{\bar\sigma: L \to E';\ \bar\sigma \text{ inj.}, \bar\sigma\restriction_K = \sigma\}$.

$$\begin{array}{ccc} L & \xrightarrow{\bar\sigma} & E' \\ | & & | \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Dann: (1) $\#\Sigma \le [L:K]$
(2) $x_1, \dots, x_n$ sep. $|K$, $E'|K'$ normal, $\Sigma \neq \emptyset$
$\Rightarrow \#\Sigma = [L:K]$.

Bew.: (1): VI nach n: $n = 0$: $L = K$, $\Sigma = \{\sigma\}$, $\#\Sigma = 1 \le 1 = [L:K]$. ✓

$n > 0$:

Betr. OE $x_1 \in L$, sei $f \in K[T]$ das Mipo von $x_1|K$.
Seien $x_1', \dots, x_t'$ die versch. Wurzeln von f^σ von E' (auch $t = 0$)

$$\overset{IV}{\Rightarrow}\left\{\begin{array}{ccc} L & \xrightarrow{\bar\sigma} & E' \\ | & & | \\ K(x_1) & \xrightarrow{\sigma_i} & K'(x_i') \\ | & & | \\ K & \xrightarrow{\sigma} & K' \end{array}\right.$$

A19.6.(2) $\rightsquigarrow$ $\forall i \le t\ \exists!$ Forts. $\sigma_i: K(x_1) \to E'$ von σ
mit $\sigma_i(x_1) = x_i'$

Setze $\Sigma_i := \{\bar\sigma \in \Sigma ; \bar\sigma(x_1) = x_i'\}$.

Dann: $\Sigma = \Sigma_1 \dot\cup \ldots \dot\cup \Sigma_t \Rightarrow \# \Sigma = \sum_{i=1}^{t} \# \Sigma_i$.

IVor. auf Σ_i: $\# \Sigma_i \le [L:K(x_1)]$, also

$$\# \Sigma \le t \cdot [L:K(x_1)].$$

wegen $t \le \deg f^\sigma = \deg f = [K(x_1):K]$ folgt:

$$\# \Sigma \le [K(x_1):K] \cdot [L:K(x_1)]$$
$$= [L:K(x_1)] \cdot [K(x_1):K] = [L:K].$$

(2): Sei $\Sigma \ne \emptyset$, $E'|K'$ normal, $x_1, \ldots, x_n$ sep.$|K$ $\Rightarrow \underline{\underline{t}} \overset{!}{=} \underbrace{[K(x_1):K]}_{=\deg f}$

⌜Denn: $\Sigma \ne \emptyset \Rightarrow f^\sigma$ hat mind. eine Wurzel in E'

$\underset{E' \text{ normal}}{\Rightarrow}$ f^σ zerfällt in E' in Lin. faktoren

ist sep., da $f = \mathrm{Mipo}(x_1)$ sep. ⌟

$$\begin{tikzcd}
E \arrow[r, "\tilde\sigma"] \arrow[d, dash] & E'' \arrow[d, dash] \\
L \arrow[d, dash] & \\
K(x_1) \arrow[r, "\sigma_i"] \arrow[d, dash] & K'(x_i') \arrow[d, dash] \\
K \arrow[r, "\sigma"] & K' \\
f & f^\sigma
\end{tikzcd}$$

* Für alle $i \le t$: $\Sigma_i \ne \emptyset$ ⌜mit A 19.11 (2)...⌟
* IV für Σ_i: $\# \Sigma_i = [L:K(x_1)]$.

Somit: $\# \Sigma = [L:K]$. $\square$

20.12. Satz: Sei $L = K(x_1, \ldots, x_n)$ endl. Erw. von K. Dann äquiv.:

(1) $L|K$ sep. (2) $x_1, \ldots, x_n$ sep.$|K$.

Bew.: (1) $\Rightarrow$ (2): ✓, (2) $\Rightarrow$ (1):

Sei $E|L$ normal über K (etwa $E = \mathrm{Zk}$ von $f_1 \cdots f_m$). $f_i = \mathrm{Mipo}_K(x_i)$

$$\begin{tikzcd}
L \arrow[r, dash] & E \arrow[d, equal] \\
K(x) \arrow[r, "\sigma_i"] \arrow[d, dash] & E \arrow[d, dash] \\
K \arrow[r, "id"'] & K
\end{tikzcd}$$

Sei $x \in L$,

$f \in K[T]$ das Mipo von $x|K$.

Zeige: f hat $m := [K(x):K] = \deg f$ versch. Wurzeln in E [dann x sep. ✓]

Seien $\sigma_1, \ldots, \sigma_t$ die versch. Einb. von $K(x) \to E$.

Die versch. Wurzeln von f in E sind: $\sigma_1 x, \sigma_2 x, \ldots, \sigma_t x$, $\underline{\underline{t \ge m}}$

Ferner: $t \le m = [K(x):K]$ nach L. 20.11. Also $t = m$. ⌜..., 20.11.⌟

20.13 Def.: K heißt <u>perfekt (vollkommen)</u> $:\Leftrightarrow$ Jede alg. Erw. von K ist sep.

20.14 Kor.: Körper K der Char. 0 sind perfekt.

Bew.: Sei $L|K$ alg., $x \in L$, f das Mipo von $x|K$.
Nach Kor. 20.8 ist f sep., d.h. x sep. $|K$.
Also ist $L|K$ sep., d.h. K perfekt. $\square$

20.15. Def.: $L|K$ <u>einfach</u> $:\Leftrightarrow \exists x \in L : L = K(x)$, x heißt <u>primitives El.</u>

20.16. <u>Satz vom primitiven Element:</u>
Jede endliche separable Körpererw. $L|K$ ist einfach,
d.h. $\exists x \in L : L = K(x)$.

Bsp.: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (T^2-2, T^2-3)
$\mathbb{Q}(\sqrt{2}+\sqrt{3})$ | sep.
$\mathbb{Q}$

<u>Bew.:</u> Seien $\sigma_1, \dots, \sigma_m$ die versch. Einb. von $K(x,y) \to E$ mit $\sigma_i \restriction K = id_K$.

$$\begin{tikzcd} E & \\ K(x,y) \arrow[u, dash] \arrow[r] \arrow[dr, dash, "\text{sep.}"'] & E \text{ (normal)} \\ K \arrow[ur, dash] & \end{tikzcd}$$

Nach L. 20.11 gilt:
$m = [K(x,y):K]$.
Die Paare $(x_1, y_1) = (\sigma_1 x, \sigma_1 y), \dots, (x_m, y_m) = (\sigma_m x, \sigma_m y)$
$\sigma_1 = id_{K(x,y)}$ sind pwv.

<u>1. Fall: K unendlich</u>

Es gibt ein $c \in K$: $\underbrace{x_1 + cy_1}_{=:z_1}, \underbrace{x_2 + cy_2}_{=:z_2}, \dots, \underbrace{x_m + cy_m}_{=:z_m}$ <u>pwv.</u>

⌜Denn: $z_i = z_j$, $i \neq j$, für höchstens ein $c \in K$
<u>K unendl.</u> $\Rightarrow \exists c \in K : z_1, \dots, z_n$ p.w.v.⌟

$$\begin{tikzcd} K(x,y) & K(z) \arrow[l, "\sigma_i"'] \\ & K \arrow[ul, dash] \arrow[u, dash] \end{tikzcd}$$

Setze $z := z_1 = x_1 + cy_1$, dann $K(x,y) \overset{\supseteq \checkmark}{=} K(z)$:

$$m \left(\begin{array}{l} K(x,y) \\ \mid \leftarrow 1 \\ K(z) \\ \mid \leftarrow m \\ K \end{array} \right.$$

L. 20.11. $\Rightarrow m \leq [K(z):K]$ nach Konstr. von z und z
⌜$\sigma_i|K(z)$ $(z) = z_i$ $\Rightarrow \sigma_1|K(z), \dots, \sigma_m|K(z)$ versch.⌟ $\square$

A21: Endliche Körper

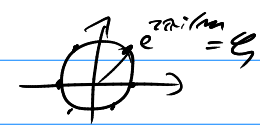
Hatten: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p prim

21.1. Einleitung: Finden alle endl. Körper! $\to \mathbb{F}_{p^n}$

Endliche Körper sind perfekt!

21.2. Satz: Endliche U Gen der mult. Gr. eines (nicht notw. endl.) Körper K sind stets zyklisch.

Bsp. in $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ etwa m-te-Einheitswurzeln $\rightsquigarrow$ zyklisch!



Bew.: Sei $U \subseteq K^\times$ endl. der Ordnung $n > 1$.

HSe.e.ab. Gr. $\rightsquigarrow U = U_1 \times \ldots \times U_m$,

die U_i sind p_i-Gruppen $\neq e$,

die $p_1, \ldots, p_m \in \mathbb{N}$ prim. pwV.

Zeige: Alle U_i sind zyklisch (dann U zykl.)

* Sei $\emptyset \neq U$ eine p-Gruppe, d.h. $\exists e > 1 : \# U = p^e$. [$U$ zykl. für $e = 1$]

Ann.: U nicht zykl. [Dann HSe.e.ab. Gr.

$U = C_1 \times \ldots \times C_r$, die C_i zykl. p-Gruppe.

und $p^e = p^{e_1} \cdot p^{e_2} \cdot \ldots \cdot p^{e_r}$, die $e_i < e$, da U nicht zykl.

Sei $e' := \max\{e_i\} < e$. $\Rightarrow \forall x \in U : x^{p^{e'}} = 1$

$\Rightarrow \forall x \in U : x^{p^{e-1}} = 1$.

Dann: $f = T^{p^{e-1}} - 1$ hat $p^e > \deg f = p^{e-1}$ versch. Wurzeln $\lightning$ A14.13.]

Also: $r = 1$.

* Seien $\# U_i = p_i^{e_i}$, $U_i = \langle a_i \rangle$, $\operatorname{ord}(a_i) = p_i^{e_i}$.

Sei $0 \neq a = a_1 \cdots a_m \in U$. Dann $\operatorname{ord}(a) = \operatorname{kgV}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_m))$

$= p_1^{e_1} \cdots p_m^{e_m} = \# U$.

Also: $U = \langle a \rangle$.

$\square$

Endl. Körper $\Rightarrow$ PZ-Charakteristik

[K unendl. $\Leftarrow$ $\mathbb{Q} \subseteq K$ $\Leftarrow$ Char K = 0]

$$p \cdot 1 = \underbrace{1 + \overbrace{1 + \ldots + 1}^{p\text{-mal}}}_{} = 0$$

21.3. Lemma: Sei K Körper, Char K = p > 0 prim. Dann:

$\sigma : K \to K$, $a \mapsto a^p$ ist inj. Endomorphismus.

K endl., Char K = p $\Rightarrow$ σ Auto.

Bew: Endo: $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$ ✓

$$\sigma(a+b) = (a+b)^p = \sum_{i=0}^{p} \underbrace{\binom{p}{i}}_{=0 \text{ für } 1 \le i \le p-1} a^i b^{p-i} = a^p + b^p = \sigma(a) + \sigma(b) \checkmark$$

in Char K = p !

Da für $1 \le i \le p-1$ gilt

$$p \mid \binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdot\ldots\cdot 2\cdot 1} \in \mathbb{N}$$

p kann nicht gekürzt werden!

Inj.: $\operatorname{Ker} \sigma = 0$, da $0, K$ einzige Ideale in K.

$\square$

21.4. Def.: Der inj. Endo σ in 21.3 heißt Frobenius-Endo.

Falls K endl., heißt σ der Frobenius-Automorphismus.

der "Frobenius" ....

nächstes Mal: $\mathbb{F}_4$, ...