FFC 3.3.2008 ①

Frobenius-Homomorphismus:

Lemma: "freshman's dream" In Komm. Ring $R$ mit $\chi(R)=p$ gilt für $a,b\in R$
$(a+b)^p = a^p + b^p$

Bew: Binom LS: $(a+b)^p = a^p + \sum_{1\le k<p} \binom{p}{k} a^k b^{p-k} + b^p$ und für
$1<k<p$ ist $\binom{p}{k}$ eine durch $p$ teilbare ganze Zahl

Kor: $K$ Körper mit $\chi(K)=p$ dann $\varphi: K\to K$ $\varphi(x)=x^p$ ein injektiver
Endomorphismus von $K$.

Homom: $(a+b)^p = a^p + b^p$ ; $(ab)^p = a^p\cdot b^p$ ✓

Inj: allg: ein Ringhom $\varphi: K\to R$ ($K$ Körper) ist entweder injektiv
oder konstant 0, weil $\mathrm{Ker}\,\varphi$ Ideal von $K$, einzige Ideale von
$K$ sind $(0)$ ($\to \varphi$ injektiv) und $K$ ($\to \varphi$ konstant 0).
Dieses $\varphi$ mit $\varphi(x)=x^p$ nicht konstant $=0$, da $\varphi(1)=1$

Bem: $\varphi: K\to K$ mit $\varphi(x)=x^p$ wobei $\chi(K)=p$ heißt Frobenius-Hom.

Bem: Frobenius Hom nicht immer surjektiv:
zB: $\varphi: \mathbb{Z}_p(x)\to\mathbb{Z}_p(x)$ nicht surj, $x$ ist kein $p$-te Potenz.

Bem: $K$ endl. Körper mit $\chi(K)=p$, dann Frobenius Hom $\varphi: K\to K$, $\varphi(x)=x^p$ Autom.
($K$ endl. $\varphi: K\to K$ inj $\Rightarrow$ endl. surj.)

Lemma: $K$ Körper, $f: K\to K$ Autom von $K$, dann $Fix(f) = \{k\in K : f(k)=k\}$
bilden Körper (Ü).

Lemma: Sei $K$ endl. Körper mit $q$ Elementen ($|K|=q$) dann gilt $\forall a\in K$
$a^q=a$ [insb gilt in $\mathbb{Z}_p$ $a^p=a$]

Bew: für $a=0$ $0^q=0$ sowieso, für $a\neq 0$ gilt $a$ Einheit
Einheitengruppe $(K\setminus\{0\},\cdot)=G$ Gruppe mit $|G|=q-1$. Für
jedes Element gilt $a^{q-1}=1$ daher $a^q=a$

Satz: Sei $K$ Körper mit $|K|=q$ $\forall n\in\mathbb{N}_{\geq 1}$ Dann ~~gilt~~ $\exists$ $F$ Körper mit
$K\subseteq F$, $|F|=q^n$ [insb. folgt aus der Existenz eines Körpers
mit $p$ El. die Existenz eines Körpers mit $p^n$ El für bel. $n$]

Bew: Sei $F$ Zerfällungskörper von $X^{q^n}-X$ über $K$. Sei $N=\{a\in F \mid a^{q^n}=a\}$ die Menge der Nullstellen von $X^{q^n}-X$ in $F$. Da $N$ die Menge der Fixpunkte von $\varphi^n=\varphi\circ\dots\circ\varphi$ ($\varphi$.. Frobenius-Hom) ist $N$ Körper. Da $\forall a\in K$ gilt $a^q=a$ und durch iterieren $a^{q^n}=a$ folgt $K\subseteq N$. Also ist $N$ Körper mit $K\subseteq N$, $N$ erzeugt von $K$ und Nullstellen von $X^{q^n}-X$, sodass $X^{q^n}-X$ über $N$ zerfällt. Daher $N=F$ Zerfällungskörper von $X^{q^n}-X$ über $K$. Außerdem hat $X^{q^n}-X$ in $N$ keine mehrfache Nullstelle, da $(X^{q^n}-X)'=q^nX^{q^n-1}-1=-1$ ($\chi(K)=p$, $q$ Potenz von $p$) Also hat $X^{q^n}-X$ in seinem Zerfällungskörper $q^n$ verschiedene Nullstellen $\to |N|=q^n$, $N=F$ hat $q^n$ Elemente. ✓

Satz: $F$ Körper, $G$ endl. Untergruppe von $(F\setminus\{0\},\cdot)$. Dann $G$ zyklisch.

Kor: Insb. gilt für jeden endl. Körper $K$ $(K\setminus\{0\},\cdot)$ zyklisch

1. Beweis: $G$ endl. Abelsche Gruppe, nach Struktursatz

$G\cong \mathbb{Z}_{m_k}\times\mathbb{Z}_{m_{k-1}}\times\dots\times\mathbb{Z}_{m_1}$ $\quad m_1|m_2|\dots|m_{k-1}|m_k$. Sei $|G|=n$

wahr aber irrelevant

da für jede $g\in G$ gilt $g^n=1$ ist eben jede $g\in G$ Nullstelle von $x^n-1$ in $F$.

da für jede $g\in G=\mathbb{Z}_{m_k}\times\dots\times\mathbb{Z}_{m_1}$ gilt $g^{m_k}=1$ ist jede $g\in G$ Nullstelle von $X^{m_k}-1$ also $|G|\le m_k$, gleichzeitig $|G|=m_k\cdot m_{k-1}\cdot\ldots\cdot m_1 \Rightarrow |G|=m_k$

daher $G=\mathbb{Z}_{m_k}$

Bem: $D$ Integr. bereich $f\in D[x]$, dann hat $f$ in $D$ höchstens $\deg f$ Nst.

2. Beweis: verwende wieder $\forall d\in\mathbb{Z}$ hat $x^d-1$ höchstens $d$ Nullstellen in $F$, also in $G$ höchstens $d$ El mit $g^d=1$. Daher hat $G$ für jeden Teiler $d\,|\,|G|$ höchstens eine zykl. Gruppe der Ord. $d$. Daher hat $G$ für jeden Teiler $d\,|\,|G|$ höchstens $\varphi(d)$ El der Ordnung $d$.

Da $|G|=\sum_{d||G|}\#\{g\in G \mid \operatorname{ord} g=d\}\le\sum_{d||G|}\varphi(d)=|G|$

Also Gleichheit die nur gelten kann, wenn $\forall d\,|\,|G|$ die Anzahl der $g\in G$ mit $\operatorname{ord} g=d$ genau $\varphi(d)$ ist. Insb. hat $G$ $\varphi(|G|)>0$ El der Ord. $|G|$ und $G$ ist zyklisch.

Kor: $K$ endl. Körper mit $|K| = q = p^n$ ($p$ prim), dann $\exists u \in K$ mit $K = \mathbb{Z}_p[u]$ (d.h. $K = \mathbb{Z}_p$ ist einfache algebr. Erweiterung).

Bew: wähle $u$ als Erzeuger von $(K\setminus\{0\}, \cdot)$ $u$ alg. über $\mathbb{Z}_p$, da $u^q - u = 0$, $u$ erzeugt $K$ über $\mathbb{Z}_p$, da $0 \in \mathbb{Z}_p$ und jedes $a \in K\setminus\{0\}$ ist Potenz von $u$.

Kor: $E \subseteq F$ endl. Körper $\Rightarrow \exists u \in F: F = E[u]$. (wähle $u$ als Erzeuger von $(F\setminus\{0\}, \cdot)$).

Kor: $E$ endl. Körper $n \in \mathbb{N}$. Dann $\exists$ irred Polynom. $f \in E[x]$ mit $\deg f = n$.

Bew: betrachtet $F:E$ mit $[F:E] = n$ $[|E| = q, |F| = q^n]$. Da $F = E[u]$ folgt $[F:E] = \deg f$. $f$ Minimalpolynom von $u$ über $E$. (Satz ü. einf. alg Körpererw.)

Werden in Kürze sehen, dass es für jede Primzahlpotenz $p^n$ (bis auf Isomorphie) genau einen Körper mit $p^n$ El. gibt. Vorhergehendes Korollar gibt eine Darstellung des Körpers mit $p^n$ El. als $K = \mathbb{Z}_p[x]/(f)$ mit $f$ bel irred $\in \mathbb{Z}_p[x]$ mit $\deg f = n$. Rechnen mit Körperel. wie mit Polynomen (Add, Mult.) und Rest mod $f$ mit $r < \deg f$ bilden El. von $K$ dargestellt als Repräsentantensyst: $\{g \in \mathbb{Z}_p[x] \mid \deg g < n\}$ sind Rep.sys. von $K = \mathbb{Z}_p[x]/(f)$

## Fortsetzbarkeit von Körperisomorphismen

Lemma: Seien $K, F$ Körper, $\varphi: K \to F$ Körperisom. dann $\bar\varphi: K[x] \to F[x]$ mit $\bar\varphi(a_0 + a_1 x + \ldots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$ Isomorphismus der Polynomringe und $\bar{\bar\varphi}: K(x) \to F(x)$ def durch $\bar{\bar\varphi}\left(\frac{f}{g}\right) = \frac{\bar\varphi(f)}{\bar\varphi(g)}$ Isom. der Körper der rat. Funktionen. [Bezeichne oft $\bar\varphi, \bar{\bar\varphi}$ einfach als $\varphi$].

Bew Skizze: $\bar\varphi$ Einsetzhomo mit $\bar\varphi|_K = \varphi$, $\bar\varphi(x) = x$. offensichtl ist $\bar\varphi$ bijektiv.

Da $\bar\varphi$ bildet alle El von $K[x]\setminus\{0\}$ auf Einheiten in $F(x)$ ab.

($\bar\varphi$ als Homom $K[x] \to F(x) \supseteq F[x]$ betrachten) Daher $\bar\varphi$ fortsetzbar zu Hom $\bar{\bar\varphi}: K(x) \to F(x)$ [$K(x)$ ist Quotientenkörper $(K[x]\setminus\{0\})^{-1}K[x]$ v. $K(x)$]

wobei die ~~Fortsetzbarkeit~~ Fortsetzung $\bar{\bar\varphi}\left(\frac{f}{g}\right) = \frac{\bar\varphi(f)}{\bar\varphi(g)}$ ist $\bar{\bar\varphi}$ injektiv da $\bar\varphi$ injektiv. Surj: jedes El von $F(x)$ ist der Form $\frac{\varphi(a_0) + \varphi\ldots + \varphi(a_n)x^n}{\varphi(b_0) + \ldots + \varphi(b_m)x^m}$, da $\varphi$ surjektiv $\to F$

Fortsetzbarkeit v. Isom auf einf. transz. Erweiterungen

Prop: $K, F$ Körper $\varphi: K \to F$ Körperisom. $K \subseteq E$, $F \subseteq L$ Körpererw. mit $u \in E$ transzendent über $K$ und $v \in L$ transz. über $F$ dann $\exists!$ Isom. $K(u) \cong F(v)$ via $\overline{\varphi}: K(u) \to F(v)$ mit $\overline{\varphi}|_K = \varphi$ und $\overline{\varphi}(u) = v$

Bew: nach Satz ü. einf. transz. Körpererw.

$\exists\, \psi: K(x) \to K(u)$ mit $\psi|_K = id$ $\psi(x) = u$, analog

$\exists\, \Theta: F(x) \to F(v)$ mit $\Theta|_F = id$ $\Theta(x) = v$

$K(u) \xrightarrow{\psi^{-1}} K(x) \xrightarrow{\varphi} F(x) \xrightarrow{\Theta} F(v)$ dann gewünschte Isom. $\Theta \circ \varphi \circ \psi^{-1}: K(u) \to F(v)$

Satz: Fortsetzbarkeit v. Isom auf einf. alg. Erweiterungen.

$K, F$ Körper $K \subseteq E$, $F \subseteq L$ Körpererweiterung $\varphi: K \to F$ Körperisom.

$u \in E$ Nullstelle von $f$ irred $\in K[x]$, $v \in L$ Nullstelle von $\varphi(f) \in F[x]$

Dann $\exists!$ Isomorph. $\overline{\varphi}: K[u] \to F[v]$ mit $\overline{\varphi}|_K = \varphi$ und $\overline{\varphi}(u) = v$.

Bew: Da $f$ irred $\Rightarrow$ $f$ bis auf mult. Konstante $\in K \setminus \{0\}$ gleich Minimalpolynom von $u$ ü. $K$. $f$ erzeugt dasselbe Ideal von $K[x]$ wie das Minimalpolynom von $u$ ü. $K$.

$f$ irred., $\varphi: K[x] \to F[x]$ Isom $\Rightarrow$ $\varphi(f)$ irred, daher erzeugt $\varphi(f)$ dasselbe Ideal von $F[x]$ wie das Minimalpolynom von $v$ über $F$. Nach Satz über einfache alg. Körpererw.: $K[u] \xrightarrow{\psi^{-1}} K[x]/(f) \xrightarrow{\tilde{\varphi}} F[x]/(\varphi(f)) \xrightarrow{\Theta} F[v]$

$\exists\, \psi: K[x]/(f) \to K[u]$ Isom mit $\psi(k + (f)) = k$ und $\psi(x + (f)) = u$

$\exists\, \Theta: F[x]/(\varphi(f)) \to F[v]$ mit $\Theta(a + (\varphi(f))) = a$ $\forall a \in F$ und $\Theta(x + (\varphi(f))) = v$

Außerdem ist $\tilde{\varphi}: K[x]/(f) \to F[x]/(\varphi(f))$ def durch $\tilde{\varphi}(g + (f)) = \varphi(g) + (\varphi(f))$ ein Isomorphismus (weil $\varphi: K[x] \to F[x]$ Isom. und allg, wenn $\varphi: R \to S$ Ring iso und $I \trianglelefteq R$ dann $\tilde{\varphi}: R/I \to S/\varphi(I)$ def durch $\tilde{\varphi}(r + I) = \varphi(r) + \varphi(I)$ ein Ring iso).

Schließlich ist $\overline{\varphi} = \Theta \circ \tilde{\varphi} \circ \psi^{-1}: K[u] \to F[v]$ Isomorphismus mit $\overline{\varphi}|_K = \varphi$ und $\overline{\varphi}(u) = v$.

Satz: $K, F$ Körper, $\varphi: K \to F$ Körperiso. $f$ irred $\in K[x]$
$E$ Zerfällungskörper von $f$ über $K$, $L$ Zerfällungskörper von $\varphi(f)$
über $F[x]$. Dann $\exists\ \overline{\varphi}: E \to L$ Isom. mit $\overline{\varphi}|_K = \varphi$