9.4.08 FFC

Gruppe der n-ten EW - zyklisch in einem Körper sind, ist die Existenz von n-verschiedenen n-ten EW äquivalent zur Existenz einer primitiven n-ten EW.
n-te Kreisteilungskörper ü. K ist def als Zerf.kö von x^n-1 über K;
wenn $\chi(k) \nmid n$, dann im n-ten Kreisteilungskörper ü. K n verschied EW (davon $\varphi(n)$ verschiedene); wenn $p = \chi(k) \mid n$ dann $n = p^k m$ mit $p \nmid m$, $x^n-1 = (x^m-1)^{p^k}$ und in n-ten Kreisteilungskörper über K nur m verschied n-te EW, nämlich nur die m-ten EW [n-te Kreisteilungskörper ist gleich dem m-ten Kreisteilungskörper f. $n = m p^k$, $p = \chi(k) \nmid m$]. Wenn $\nmid \chi(k) = p \nmid n$, dann sei F der n-te Kreisteilungskörper ü. K und $\varphi_n = \prod_{\text{primitive n-te EW in } F} (x-\omega)$, dg $\varphi_n = \varphi(n)$ Induktives Verfahren die Kreisteilungspolyn. zu konstruieren, aus dem hervorgeht, dass die Koeff der φ_n in Primring ($\mathbb{Z}_p$ bzw $\mathbb{Z}$) liegen: $x^n-1 = \prod_{d \mid n} \varphi_d(x)$ $\varphi_1(x) = x-1$
$x^n-1 = \varphi_n(x) \prod_{\substack{d \mid n \\ d<n}} \varphi_d(x)$ Nach IV. hat $g(x) = \prod_{\substack{d \mid n \\ d<n}} \varphi_d$ Koeff in Primring

x^n-1, φ_n, $g(x)$ normiert. Allg. $R \subseteq S$ kommR Rig mit 1 f,g,h ~~normiert~~ $\in S[x]$
h normiert $f,g \in R[x]$ $f(x) = g(x)h(x) \Rightarrow g \in R[x]$
und wenn φ_d für $d<n$ schon konstruiert, $\varphi_n = \frac{x^n-1}{\prod_{\substack{d \mid n \\ d<n}} \varphi_d(x)}$

[in $\mathbb{Q}$ sind die Kreisteilungsp. irred.]
$\mathbb{Z}_p \subseteq \mathbb{F}_q$ Kreisteilungspolynome $\in \mathbb{Z}_p[x] \subseteq \mathbb{F}_q[x]$ über $\mathbb{F}_q$ zerfällt φ_n $p \nmid n$ in irred Faktoren von Grad (= Grad der Körpererw, wenn man eine primitive n-te EW adjungiert) m mit m minimal sod $n \mid q^m-1$

Konkrete Darstellung von endlichen Körpern
f bel. irred $\in \mathbb{Z}_p[x]$ grad $f = m$ dann $\mathbb{Z}_p[x]/(f) \simeq \mathbb{F}_{p^m}$
[genauso $\mathbb{F}_q$ endl. Körper $f \in \mathbb{F}_q[x]$ irred, dg $f = m$ dann $\mathbb{F}_q[x]/(f) \simeq \mathbb{F}_{q^m}$]
Rechnet in $\mathbb{Z}_p[x]/(f) = \mathbb{F}_{p^m}$ so: Restklassen mod p Addieren und multiplizieren;
Repräsentantensyst bestehend aus alle $g \in \mathbb{Z}_p[x]$ mit dg $g < m$.

~~Wenn~~ f

f irred $\in \mathbb{F}_q[x]$ mit $\deg f = n$ heißt primitiv, wenn eine Nullstelle α von f in $\mathbb{F}_q[\alpha]$ die Multiplikative Gruppe erzeugt. [wg. das für eine Nullstelle gilt, dann für alle, wg Isom. $\mathbb{F}_q[\alpha] \cong \mathbb{F}_q[\beta]$ $\alpha \mapsto \beta$ für Nullstelle α, β der selben irred Poly $\in \mathbb{F}_q[x]$) Wenn $f \in \mathbb{F}_q[x]$ primitiv, dann $x+f$ Erzeuger von $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^n}$ ($n = \deg f$).

Potenzen von $x+f = \bar{a}$ auflisten $\bar{1}, \dots, \bar{a}^{q^n-2}$ für $\bar{a}^n, \dots \bar{a}^{q^n-2}$ Rest mod f bilden, in Tabelle, dann hat man Darstellung der El des Körpers, die sowohl für Addition (Poly. vom Grad $< n$) als auch f. Multiplikation (Potenz von $\bar{a}$, Exponent mod q^n-1) praktisch sind.

Da $\mathbb{F}_{q^n}$ der (q^n-1)-te Kreisteilungskörper von $x^{q^n-1}-1$ über $\mathbb{F}_q$ ist, ist jeder irred Faktor von q_{q^n-1} ein primitives Polynom.

Matrixdarstellung: alg. Elsbeth

Allgemein: K Körper $\subseteq$ Algebra (Ring mit $1_A = 1_K$ ist K-VR) $a \in A$ heißt

$K[a] \cong K[x]/f$ über f Minimalpolynom von a, d.h. normierter Erzeuger des Ideals $\{g \in K[x] \mid g(a) = 0\} \trianglelefteq K[x]$

[i.A. Minimalp. nicht irred.].

f normiert in $K[x]$, dann $K[x]/(f) = K[a]$ weiters isomorph zu der Gefährtenmatrix C_f vom erzeugten Unterring von $M_n(K)$ ($n = \deg f$).

Wobei $C_f = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & \ddots \\ -a_0 & a_1 & \dots & -a_{n-1} \end{pmatrix}$; dieser Unterring ist auch isom. zu $K[x]/(f)$

a: Koeff von f.

da f das Minimalpolynom von C_f ist.

Offenbar ist das Charakteristische Poly. von C_f gleich f aber auch das Minimalp. (erzeuger des Ideals $\{g \in K[x] \mid g(C_f) = 0\}$

Allg: Satz von McCoy:

R kommR Ring $C \in M_n(R)$, dann ist das Ideal $\{f \in R[x] \mid f(C)=0\}$

gleich $(F_0(xI-C) : F_1(xI-C)) = \{f \in R[x] \mid \forall g \in F_1(xI-C): f \cdot g \in F_0(xI-C)\}$

wobei für $k=0,\dots,n$ $F_k(M)$ (M Matrix mit Einträgen in S)

das von den $(n-k)\times(n-k)$ Minoren erzeugte Ideal von M ist.

$M \in M_n(S)$ (S kommR Ring) $n-k \times n-k$ Minor von M ist eine Determinante

eine $n-k \times n-k$ Untermatrix von M (einer Matrix die aus M durch

Streichung von k Zeilen u. k Spalten entsteht.)

Insb: $F_0 = (\det M) \cdot S$ das von der $\det M$ erz. Hauptideal von S;

F_{n-1} das von den Einträgen von M erz. Ideal von S.

Bem: Elementare Zeilen u. Spalten Operationen [Addition des s-fach ($s \in S$) einer

Zeile i zur Zeile j ($j \neq i$) analog für Spalten) ändern nicht an

$F_0, F_1, \dots F_{n-1}, F_n$.

$$C_f = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 0 \; 1 \\ -a_0 & \cdots & & -a_{n-1} \end{pmatrix} \quad xI - C_f = \begin{pmatrix} x & -1 & & \\ & x & -1 & \\ & & \ddots & \ddots \\ & & & x \; -1 \\ a_0 & a_1 & \cdots & x+a_{n-1} \end{pmatrix}$$