FFC 230408

$a \in S$ Ring, R komm Ring $\subseteq S$. Wenn a Nullstelle eines normierten Poly $f \in R[x]$ ($\deg f = n$), dann besteht der von a über R erzeugte Unterring von S (a priori $R[a]$) aus R-Linear Kombination von $1, a, a^2 \dots a^{n-1}$; und ~~dann~~ wenn $f \in R[x]$ von minimalen Grad mit $f(a) = 0$, dann Darst eind.

$f = x^n + b_{n-1}x^{n-1} + \dots + b_0$ dann $a^n = -b_{n-1}a^{n-1} - \dots - b_0$ a^n und induktiv alle höhen Potenzen von a als R-Linearkomb von $1, a, \dots a^{n-1}$ darstellbar. Wenn zwei Darstellungen dann Subtraktion gibt Polynom vom Grad $\leq n-1$ mit a als Nst.

Berlekamp - Alg zur Faktorisierung von Polynomen über endl. Körpern

Wollen $f \in \mathbb{F}_q[x]$ in irred Polynome faktorisieren.

Lemma: Sei $f \in \mathbb{F}_q[x]$ gg. Wenn $g \in \mathbb{F}_q[x]$ sod $f \mid g^q - g$ dann $f = \prod_{c \in \mathbb{F}_q} ggT(f, g-c)$. Wenn zusätzlich $\deg g \neq 0$ $\deg g < \deg f$, dann ist diese Faktorisierung von f nicht trivial, d.h. die Faktoren sind nicht konst Einheiten und ein zu f ~ Polynom.

Bew: in $\mathbb{F}_q[x]$: $x^q - x = \prod_{c \in \mathbb{F}_q}(x-c)$, also $\forall g \in \mathbb{F}_q[x]$ $g^q - g = \prod_{c \in \mathbb{F}_q}(g-c)$

Die $g-c$ sind für verschiedene c paarweise rel. prim.

Wenn $f \mid g^q - g$ dann $f = ggT(f, g^q - g) = ggT(f, \prod_{c \in \mathbb{F}_q} g-c) \overset{!}{=} \prod_{c \in \mathbb{F}_q} ggT(f, g-c)$

weil die Faktoren $g-c$ paarweise rel prim, Der Fall $f \mid g-c$ für ein c kann nur vorkommen, wenn $\deg g = \deg(g-c) \geq \deg f$ oder wenn $g-c=0$ (d.h. g konstant) □

Lemma: $f \in \mathbb{F}_q[x]$, $f = f_1^{k_1} \cdots f_s^{k_s}$ wobei $f_1 \dots f_s$ verschiedene irred Polynome sind, dann ist die Anzahl der $g \in \mathbb{F}_q[x]$ mit $f \mid g^q - g$ und $\deg g < \deg f$, genau q^s.

Bew: wenn $f \mid g^q - g = \prod_{c \in \mathbb{F}_q} g-c$ dann $\forall f_i$ $\exists! c \in \mathbb{F}_q$ mit $f_i^{k_i} \mid g-c$.

Umgekehrt, wenn $\forall f_i$ $\exists c$ mit $f_i^{k_i} \mid g-c$ dann $f \mid \prod_{c \in \mathbb{F}_q} g-c = g^q - g$.

(die $f_i^{k_i}$ für versch. i rel. prim.)

Für jede Wahl von $(c_1,\dots,c_s)\in \mathbb{F}_q^s$ $\exists!\, g\in \mathbb{F}_q[x]$ mit $f_i^{k_i} \mid g-c_i$ und $\deg g < \deg f$, weil nach Chin RS: $g \equiv c_i$ mod $f_i^{k_i}$ $(1\le i\le s)$ lösbar, und eind lösbar mod $\prod_{i=1}^{s} f_i^{k_i} = f$

Also gibt es genau q^s solche g, für jede Wahl von $(c_1,\dots,c_s)$ einen. □

Def: Ein $g\in \mathbb{F}_q[x]$ mit $f \mid g^q-g$ und $0<\deg g<\deg f$ heißt f-reduzierend

Da unter den q^s Polynome g mit $f\mid g^q-g$, $\deg g<\deg f$ alle q Konstanten $\in \mathbb{F}_q$ vorkommen, gibt es zu $f\in\mathbb{F}_q[x]$ genau q^s-q f-reduzierende Polynome, wobei s = Anzahl der verschiedenen Faktoren von f.

Satz: Berlekamp Algo zum Finden derjenigen g mit $\deg g<\deg f$ und $f\mid g^q-g$:

Division mit Rest von x^{jq} für $j=0,\dots,n-1$ ($n=\deg f$) durch f:

$x^{jq} = f(x)\cdot h_j(x) + r_j(x)$, $r_j(x) = b_{j0}+b_{j1}x+\dots+b_{j,n-1}x^{n-1}$

Matrix $B=(b_{jk})_{\substack{0\le j\le n-1\\ 0\le k\le n-1}}$

$g=c_0+c_1x+\dots+c_{n-1}x^{n-1}$ erfüllt $f\mid g^q-g$ genau dann, wenn

$(c_0\dots c_{n-1})\cdot(B-I) = 0$ ist.

Bew: Sei $g=c_0+c_1x+\dots+c_{n-1}x^{n-1}$ erfülle $\deg g<\deg f$ ~~$f\mid g^q-g$~~. Da $g^q = c_0+c_1x^q+\dots+c_{n-1}x^{(n-1)q}$

ist $g^q-g\equiv 0$ mod f äquivalent zu $c_0 r_0(x)+\dots+c_{n-1}r_{n-1}(x)-(c_0 1+c_1x+\dots+c_{n-1}x^{n-1})$ $\equiv 0$ mod f da Grad der vorkommenden Polyn $<\deg f$, ist in diesem Fall $\equiv 0$ mod f äquiv zu $=0$ in $\mathbb{F}_q[x]$, d.h. äquiv. zu:

$c_0b_{00}-c_0+c_1b_{10}+c_2b_{20}+\dots+c_{n-1}b_{n-1,0}=0$ [Koeff von x^0]

$c_0b_{0k}+c_1b_{1k}+\dots+c_kb_{kk}-c_k+c_{n-1}b_{n-1,k}=0$ [Koeff von x^k]

d.h. $(c_0,c_1,\dots,c_{n-1})\cdot(B-I)=0$

Beim Lösen d. lin Gl. sys findet man die Dimension des Lösungsraums: q^s und erhält dabei s: Anzahl der versch Faktoren von f. Als Lösungen erhält man (wenn $s>1$), nach ~~wegst~~ Wegwerfen der Konstanten, q^s-q f-reduzierende Polyn.