Adjungieren einer Nullstelle, Zerfällungskörper eines Polynoms

Satz: Sei $f \in K[x]$, $\deg f \geq 1$. Dann $\exists F:K$ Körpererweiterung mit $[F:K] \leq \deg f$, bzw. $[F:K] = \deg f$ wenn f irreduzibel $\in K[x]$, sodass f in F eine Nullstelle u hat und $F = K[u]$

Bew: o.BdA f irred, sonst irred Fakt von f verwenden.

Sei $F = K[x]/(f)$. Da f irred ist (f) maximales Ideal ($K[x]$ Hauptidealring). (f) max Ideal in $K[x] \Leftrightarrow K[x]/(f) = F$ Körper.

(Eine Isomorphe Kopie von K ist enthalten in F: $\varphi: K[x] \to K[x]/(f)$ kanon. proj. dann $\varphi|_K : K \to F$ injektiv. $\operatorname{Ker} \varphi = (f)$, $\operatorname{Ker}\varphi \cap K = \{0\}$ d.h. $\operatorname{Ker} \varphi|_K = \{0\}$.

K eingebettet in F als El. der Form $k + (f)$, $\cancel{\forall}$ $k \in K$

Nullstelle von f in F ist $x + (f)$. Nämlich:

$f(x+(f)) = f(x) + (f) = f + (f) = (f) = 0 + (f) = 0_F$

F wird als Ring von $K \cup \{x\}$ erzeugt, da $K[x]$ von $K \cup \{x\}$ erzeugt wird und $F = \operatorname{Im} \varphi$, $\varphi: K[x] \to K[x]/(f) = F$ und Ringhom ein Erzeugendensyst auf Erzeugendensyst abbildet.

Def: $f \in K[x]$, f zerfällt über F (in $F[x]$), wenn in $F[x]$ gilt: (in Lin. Fakt)

$f = c \cdot (x - a_1)(x - a_2) \dots (x - a_n)$ mit $a_1 \dots a_n \in F$

Bsp: Es kann passieren, dass nach Adjungieren einer Nullstelle u das Polynom in $K[u]$ zerfällt, muss aber nicht.

n-te zyklotomisches Polynom (Kreisteilungspolynom)

$\varphi_n(x) = \prod_{\substack{1 \leq k \leq n \\ ggT(k,n)=1}} (x - e^{\frac{2\pi i}{n} k})$ $\qquad \varphi_n \in \mathbb{Z}[x]$ irred in $\mathbb{Q}[x]$

Sei w eine Nullstelle von φ_n, dann zerfällt φ_n in $\mathbb{Q}[w]$ (andere Nullst. sind Potenzen von w)

anderes Bsp: x^3-2 sei $\sqrt[3]{2}$ die reelle Nullstelle, dann
$\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, enthält nicht die beiden anderen Nullst.
f zerfällt nicht in $\mathbb{Q}[\sqrt[3]{2}]$.

Def: $f \in K[x]$, $\deg f \geq 1$, F Körper $\supseteq K$ heißt Zerfällungskörper von f über K wenn 1) f in $F[x]$ zerfällt
und 2) $F = K[u_1,\dots,u_n]$ mit $u_1,\dots,u_n$ Nullstellen von f.

Satz: $f \in K[x]$ $\deg f = n \geq 1$. Dann $\exists F$ Zerfällungskörper von f über K, mit $[F:K] \leq n!$.

Bew: Ind. $n = \deg f$. $n=1$
$f = ax+b = a(x+\frac{b}{a}) = a(x-(-\frac{b}{a}))$ mit $-\frac{b}{a} \in K$, f zerfällt über $K = K[-\frac{b}{a}]$

$n-1 \to n$ $\deg f = n > 1$, adjungieren Nullstelle u von F: in $K[u]$ gilt
$f = (x-u)g(x)$ $g(x) \in K[u][x]$, $\deg g \leq n-1$. Nach IV $\exists F$
Zerfällungskörper von g über $K[u]$, $F = K[u][u_1 .. u_n] = K[u,u_1,\dots,u_n]$
u_i Nullstelle von g, also ~~von~~ von f, g zerfällt in F
also auch f: F Zerfällungskörper von f über K

Vorschau: Zwei Arten, endl. Körper zu konstruieren, ausgehend von $\mathbb{Z}_p$ (p prim) als p-el. Körper: 1) zeigen, dass es für jedes $n \in \mathbb{N}$ ein irred. Polynom $f \in \mathbb{Z}_p[x]$ mit $\deg f = n$ gibt, dann Nullst. von f adjungieren, erhält $F = \mathbb{Z}_p[u]$ mit $[F:\mathbb{Z}_p] = n$, F n-dim $\mathbb{Z}_p$-VR $\Rightarrow F$ hat p^n Elemente.
2) F mit $[F:\mathbb{Z}_p] = n$ (und daher $|F| = p^n$) konstruieren als Zerfällungskörper von $x^{p^n}-x$ über $\mathbb{Z}_p$. Machen zuerst 2 dazu ein paar Tatsachen über mehrf. Nullst. zeigen

Mehrfache Nullstellen, formale Ableitung

Def: $f \in K[x]$, $f = a_0 + a_1 x + .. + a_n x^n$. Die (formale) Ableitung von f ist f' mit $f' = a_1 + 2a_2 x + 3a_3 x^2 + .. + n a_n x^{n-1} \overset{def}{=} \sum_{k=1} k a_k x^{k-1}$

Bem: aus $f' = 0$ folgt i. A. nicht dass f konstant ist.
z.B x^p in $\mathbb{Z}_p[x]$

Def: $f \in K[x]$, $u \in K$ heißt mehrfache Nullstelle von f, wenn $(x-u)^2 | f$ in $K[x]$, und für eine Nullstelle u von f heißt das maximale m mit $(x-u)^m | f$ die Vielfachheit der Nullstelle u.

Satz: $f \in K[x]$, $u \in K$
u ist mehrf. Nullstelle von $f \Leftrightarrow u$ Nullstelle von f und von f'

Bew: „$\Rightarrow$" $f(x) = (x-u)^2 g(x)$, $f'(x) = 2(x-u)g(x) + (x-u)^2 g'(x)$
mit Einsetzhom $f'(u) = 0$, $f(u) = 0$.
„$\Leftarrow$" ang u ist einfache Nullstelle d.h $f(x) = (x-u)g(x)$, $(x-u) \nmid g$
dann u keine Nullstelle von g
$f' = g(x) + (x-u)g'(x)$ mit Einsetzhom $f'(u) = g(u) \neq 0$

Satz: $f \in K[x]$
f hat in irgendeinem Erweiterungskörper $F \supseteq K$ eine mehrfache Nullstelle $\Leftrightarrow ggT(f, f') \neq 1$ [in $K[x]$]

Bem: $f, g \in K[x]$, dann ist der in $K[x]$ vorhandene $ggT(f,g)$ auch $ggT(f,g)$ als Polynom in $F[x]$ für jeden Körper $F \supseteq K$. Euklidischer Alg. zur Bestimmung von $ggT(f,g)$ in $K[x]$ ausgeführt ist gleichzeitig auch der Euklid. Alg. in $F[x]$

Bew d. Satzes: „$\Rightarrow$" f hat in $F \supseteq K$ mehrf. Nullst. u dann sei φ das Minimalpolynom von u über K; $f(u) = 0$, $f'(u) = 0 \Rightarrow$ ~~deg~~ $\varphi | f$, $\varphi | f'$
φ nicht konst. Polynom $\in K[x]$, das f, f' und daher $ggT(f, f')$ teilt, $ggT(f, f') \neq 1$

$\Leftarrow$ f, f' haben nicht konst. gemeinsamen Faktor g, im Zerfällungskörper von g haben f, f' gemeinsame Nullstelle, also f eine mehrf. Nullstelle

Charakteristik eines Ringes

Def: R Ring dann sei $\mathrm{Ann}_{\mathbb{Z}} R = \{k \in \mathbb{Z} \mid \forall r \in R \quad kr = 0\}$

Dann $\mathrm{Ann}_{\mathbb{Z}} R \trianglelefteq \mathbb{Z}$, daher $\exists! n \in \mathbb{N}_0 \quad \mathrm{Ann}_{\mathbb{Z}} R = n\mathbb{Z}$

Dieses n ist $\chi(R)$. $\chi(R)$ heißt Charakteristik von R.

Lemma: R nullteilerfrei $\Rightarrow$ $\chi(R) = 0$ oder $\chi(R) = p$ prim

Bew: ang. $\chi(R) = n \cdot m \quad 1 < n, m < nm$ Konstruieren Nullteiler:

Da $1 < n < \chi(R)$ $\exists r \in R \quad nr \neq 0$, analog $\exists s \in R \quad ms \neq 0$

$(nr)(ms) = (nm)(rs) = 0$ Also nr, ms Nullteiler ✓

Korrolar: insb. hat jeder Körper Charakteristik 0 oder p prim.

Def: Für Ring R mit 1 ist der Primring von R der von 1 erzeugte Unterring v. R

Für Körper K ist der Primkörper der von 1 erz. Unterkörper von K.

Lemma: R Ring mit 1 $\quad \chi(R) = 0 \Rightarrow$ Primring $\cong \mathbb{Z}$

$\chi(R) = n \in \mathbb{N} \Rightarrow$ Primring $\cong \mathbb{Z}_n$

K Körper $\quad \chi(K) = 0 \Rightarrow$ Primkörper $\cong \mathbb{Q}$

$\chi(K) = p \Rightarrow$ Primkörper $\cong \mathbb{Z}_p$

Da die additiven Vielfachen von 1 und -1 bzgl. Mult. abgeschlossen sind ist die von 1 erz. Ugr von $(R, +)$ ein Ring, also der kleinste Ring der 1 enthält, d.h. der Primring.

In Ring mit 1 gilt für $k \in \mathbb{Z}$

$(\forall r \in R \quad kr = 0) \Leftrightarrow k 1_R = 0$

$r = 1r$

$k(1r) = (k1) \cdot r = 0$

daher gilt ~~$\chi(R)$~~ in Ring mit 1 wenn $\chi(R) \in \mathbb{N}$, dann ist $\chi(R)$ die Ordnung von 1 in der Gruppe $(R, +)$ und wenn $\chi(R) = 0$ dann ist die Ordnung von 1 in $(R, +)$ unendlich.

Also ist der von 1 erz. Unterring im Falle $\chi(R) = n \in \mathbb{N}$ isomorph zu $\mathbb{Z}_n$ und im Falle $\chi(R) = 0$ isomorph $\mathbb{Z}$

Primkörper: Wenn $\chi(K) = p$ dann ist der von 1 erz. Ring $\mathbb{Z}_p$ also Körper, also der Primkörper; wenn $\chi(K) = 0$, dann $\mathbb{Z} \subseteq K$, wegen Fortsetzbarkeit der Inklusion $\mathbb{Z} \hookrightarrow K$ auf Quotientenkörper $\mathbb{Q}$ ist $\mathbb{Q}$ in K eingebettet und besteht aus Ausdrücken $r \cdot s^{-1}$ mit r, s aus dem Primring, der in jedem Unterkörper von K enthalten ist, also diese Kopie von $\mathbb{Q}$ Primkörper.

Kor: jeder endl. Körper hat als Charakteristik eine Primzahl p.

Endliche Körper

Kennen schon $\mathbb{Z}_p$ für p prim als Körper: jede Restklasse $\neq 0$ in $\mathbb{Z}_p$ invertierbar: $ggT(k, p) = 1 \Rightarrow \exists\, a, b \in \mathbb{Z}$ $1 = ak + bp$ in $\mathbb{Z}_p$: $1 = a \cdot k$ ~~a invers~~ a invers zu k.

Lemma: jeder endl Körper K hat p^n Elemente für ein p prim und ein $n \in \mathbb{N}$ nämlich für $p = \chi(K)$ und $n = \dim_{\mathbb{Z}_p} K$

Bew: Wissen: $\chi(K) = p$ prim, daher enthält K als ~~Primk~~ Primring eine Kopie von $\mathbb{Z}_p$ (Körper), Also K $\mathbb{Z}_p$-VR

$\dim_{\mathbb{Z}_p} K = n$ endl. (da K endl) und wenn $\dim_{\mathbb{Z}_p} K = n$ dann $|K| = p^n$ (n-el Basis, jedes El eind als $\mathbb{Z}_p$-linearkomb der Basis el. darstellbar, p^n Mögl. für die Koeff.)