UE 384 ► Übungsaufgabe 6.2.6.7. (F) Seien R und U wie in der vorigen Aufgabe. Geben Sie ein Polynom $p(x) \in U[x]$ an, welches in R die Nullstelle t hat. (Wenn Ihnen das zu leicht ist: Finden Sie so ein Polynom, welches in $U[x]$ irreduzibel ist.) **◄ UE 384**

- $R = (\mathbb{Z}/5\mathbb{Z})[t]$; $U = \bigcap \{ V \subseteq R \mid V \text{ Unterring mit 1 von } R,\ t^5 \in V \}$

  $p(x) = x^5 - t^5$ hat t als Nullstelle

- Es gilt $t^5, \bar{1}, \bar{0} \in U$, daher auch $\mathbb{Z}_5 := \mathbb{Z}/5\mathbb{Z} \subseteq U$; , $\forall n \in \mathbb{N}: t^{5n} \in U$

  Also $U = \left\{ \sum_{k=0}^{n} \alpha_k t^{5k} \mid \alpha_k \in \mathbb{Z}_5,\ n \in \mathbb{N} \right\} \overset{?}{=}$

Satz 6.3.3.3. *Die Automorphismen von* $\mathrm{GF}(p^n)$ *sind genau die Abbildungen der Form* $a \mapsto a^{p^k}$ *mit* $k = 0, 1, \ldots, n-1$ *(die sogenannten* Frobeniusautomorphismen*). Sie bilden eine zyklische Gruppe, die vom Automorphismus* $a \mapsto a^p$ *erzeugt wird.*

UE 386 ▶ Übungsaufgabe 6.3.3.4. (W) Beweisen Sie Satz 6.3.3.3, indem Sie folgendes zeigen: **◀ UE 386**

1. Ist p eine Primzahl, $k, n \in \mathbb{N}$, $n \geq 1$, so ist die Abbildung $\varphi : a \mapsto a^p$ ein Automorphismus von $\mathrm{GF}(p^n)$.

2. Die in der Automorphismengruppe $\mathrm{Aut}(\mathrm{GF}(p^n))$ von φ erzeugte Untergruppe besteht aus allen $\varphi^k : a \mapsto a^{p^k}$ mit $k = 0, \ldots, n-1$.[10]

3. Jeder Automorphismus φ eines Körpers K lässt den Primkörper P von K punktweise fest. Hinweis: P wird als Ring mit 1 von der leeren Menge erzeugt.

4. Jeder Automorphismus von $\mathrm{GF}(p^n)$ ist von der Form $a \mapsto a^{p^k}$. Hinweis: Jeder Automorphismus ist eindeutig durch seinen Wert für ein primitives Element α bestimmt. Als mögliche Werte kommen genau die Konjugierten von α in Frage. Davon gibt es n Stück, genauso viele wie Frobeniusautomorphismen.

1) Sei $p \in \mathbb{P}$, sei $n \in \mathbb{N}$, $n > 0$; $\varphi : GF(p^n) \to GF(p^n) : a \mapsto a^p$

•) „injektiv" $a, b \in GF(p^n)$ mit $\varphi(a) = \varphi(b) \Leftrightarrow a^p = b^p \Leftrightarrow a^p - b^p = 0$

Nach Satz 3.3.4.3 gilt $(a-b)^p = a^p - b^p = 0$ also $a - b = 0 \Rightarrow a = b$

•) „surjektiv" Sei $b \in GF(p^n)$ bel., ges.: $a \in GF(p^n)$: $\varphi(a) = b \Leftrightarrow a^p = b \Leftrightarrow a^p - b = 0$

daraus folgt $(a^p - b)^{p^{n-1}} = 0 \Rightarrow (a^p)^{p^{n-1}} - b^{p^{n-1}} = 0 \Rightarrow a^{p^n} - b^{p^{n-1}} = 0 \Rightarrow a = b^{p^{n-1}}$

•) „Homomorphismus" Seien $a, b \in GF(p^n)$

$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$

$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\,\varphi(b)$

2) Aus Prop. 2.1.5.2 wissen wir bereits, dass $(\mathrm{Aut}(GF(p^n)), id, \circ, ^{-1})$ tatsächlich eine Gruppe ist

Sei $G := \{\varphi^k \mid k \in \{0, \ldots, n-1\}\}$

•) $\varphi^0 = id \in G$

•) $k, l \in \{0, \ldots, n-1\}$ bel., $a \in GF(p^n)$ bel.: $\varphi^k(\varphi^l(a)) = \varphi^k(a^{p^l}) = (a^{p^l})^{p^k} = a^{p^{l+k}}$

Fall 1: „$l+k < n$" dann ist $\varphi^k(\varphi^l(a)) = a^{p^{l+k}} = \varphi^{k+l}(a)$, also $\varphi^k \circ \varphi^l = \varphi^{k+l} \in G$

Fall 2: „$l+k \geq n$" es ist $l+k \leq (n-1)+(n-1) = 2n-2$, also $\exists m \in \{0, \ldots, n-2\}$: $l+k = n+m$

dann ist $\varphi^k(\varphi^l(a)) = a^{p^{l+k}} = a^{p^{n+m}} = a^{p^n p^m} = (a^{p^n})^{p^m} = a^{p^m} = \varphi^m(a)$

also $\varphi^k \circ \varphi^l = \varphi^m \in G$

•) $k \in \{0, \ldots, n-1\}$ bel., $a \in GF(p^n)$ bel

Fall 1: „$k = 0$" $\varphi^k = id$, $(\varphi^k)^{-1} = id \in G$

Fall 2: „$k \neq 0$" $\varphi^k(\varphi^{n-k}(a)) = \varphi^k(a^{p^{n-k}}) = (a^{p^{n-k}})^{p^k} = a^{p^n} = a$, also $(\varphi^k)^{-1} = \varphi^{n-k} \in G$

Also ist G eine Gruppe also sicher $\mathrm{Aut}(GF(p^n)) \subseteq G$

Aus Prop. 6.3.3.2 Punkt 4 wissen wir $|Aut(GF(p^n))| = n$ und $|G| = n$ also $G = Aut(GF(p^n))$

3) Sei K ein Körper, φ ein Automorphismus von K, P Primkörper von K

Nach Definition ist $P = \bigcap \{L \subseteq K \mid L \text{ Unterkörper von } K\}$

Wir fassen K als Ring mit 1 auf und definieren $R = \bigcap \{L \subseteq K \mid L \text{ Unterring mit } 1 \text{ von } K\}$

Es gilt sicher $R \subseteq P$ — für $|K| = \infty$ fehlt die Argumentation!

Ist K endlich so auch $R \subseteq K$ und R ist Integritätsbereich nach Satz 3.3.2.1 ist also R Körper, daher $P \subseteq R$

Haben wir das so gilt $R = \langle \emptyset \rangle$, mit Sicherheit ist $id \in Aut(K)$ und $id|_R : R \to K$ sowie $\varphi|_R : R \to K$ sind Homomorphismen, und da $\forall a \in \emptyset : id|_R(a) = \varphi(a)$ und $R = \langle \emptyset \rangle$ gilt nach Prop. 2.3.1.13 bereits $\varphi|_R = id|_R$

4) Sei $\varphi \in Aut(GF(p^n))$ bel. Nach Satz 6.2.5.1 ist die multiplikative Gruppe von $GF(p^n)$ zyklisch, also $\exists \alpha \in GF(p^n) \setminus \{0\} : GF(p^n) \setminus \{0\} = \{\alpha^k \mid k \in \mathbb{Z}\}$

Man erkennt, dass $\{\alpha^k \mid k \in \{1, \dots, p^n - 1\}\}$ bereits eine Gruppe mit $p^n - 1$ Elementen ist ($\alpha^{p^n} = \alpha$ und $\alpha^{p^n - 1} = 1$). Sei f das Minimalpolynom von α über $GF(p)$ — warum?

Da α bereits $GF(p^n) \setminus \{0\}$ erzeugt ist $GF(p^n) = GF(p)(\alpha)$ und wegen $[GF(p^n) : GF(p)] = n$ gilt $grad(m) = [GF(p^n) : GF(p)] = n$, mit den verschiedenen Nullstellen $\alpha_1, \dots, \alpha_{n-1}, \alpha_n$

Nach Prop. 6.3.3.2 Punkt (4) gibt es zu jedem $i \in \{1, \dots, n\}$ genau einen Automorphismus mit φ_i mit $\varphi_i(\alpha) = \alpha_i$, wobei $\alpha \in \{\alpha_1, \dots, \alpha_n\}$

Sei also $\varphi(\alpha) = \alpha_\ell$, $\ell \in \{1, \dots, n\}$, so ist φ bereits eindeutig bestimmt, denn für $\beta \in GF(p^n) \setminus \{0\}$ bel. gilt $\exists m \in \{1, \dots, p^{n-1}\} : \beta = \alpha^m$ und

$\varphi(\beta) = \varphi(\alpha^m) = \varphi(\alpha)^m = \alpha_\ell^m$

Es gibt also höchstens n Automorphismen, wir haben allerdings bereits die n verschiedenen Frobeniusautomorphismen gefunden, diese müssen nun schon alle sein.

UE 391 ▶ Übungsaufgabe 6.3.3.9. (F) Sei K ein Körper der Charakteristik $p > 0$. Man zeige: ◀ **UE 391**
$x^p + a \in K[x]$ ist entweder irreduzibel, oder p-te Potenz eines linearen Polynoms.

•) Nach Satz 6.1.1.8 ist $p \in \mathbb{P}$ und der Primkörper $P \cong \mathbb{Z}_p$, hat also p Elemente, da wir aus Satz 6.3.2.2. schon wissen wie die Unterkörper eines endl. Körpers aussehen wissen wir $\exists n \in \mathbb{N}^+ : K = GF(p^n)$ und $GF(p^n)$ ist Zerfällungskörper von $q(x) = x^{p^n} - x$

$f(x) = x^p + a = x^p + a^{p^n} = x^p + (a^{p^{n-1}})^p = (x + a^{p^{n-1}})^p$ irreduzibel ?

UE 393 ▶ **Übungsaufgabe 6.3.4.3.** (B) Konstruieren Sie einen Körper mit 8 Elementen nach dem Vorbild der Konstruktion von GF(9) weiter oben. ◀ **UE 393**

·) Wir betrachten das über $\mathbb{Z}_2$ irreduzible Polynom $f(x) = x^3 + x^2 + 1$ und erhalten für α mit $\alpha^3+\alpha^2+1=0 \Leftrightarrow \alpha^3 = \alpha^2+1$ mit $\{1, \alpha, \alpha^2\}$ eine Basis von GF(8) über $\mathbb{Z}_2$

Element	Koordinaten
0	$(0,0,0)$
$\alpha^0 = 1$	$(1,0,0)$
$\alpha^1 = \alpha$	$(0,1,0)$
$\alpha^2 = \alpha^2$	$(0,0,1)$
$\alpha^3 = 1+\alpha^2$	$(1,0,1)$
$\alpha^4 = 1+\alpha+\alpha^2$	$(1,1,1)$
$\alpha^5 = 1+\alpha$	$(1,1,0)$
$\alpha^6 = \alpha+\alpha^2$	$(0,1,1)$

Stimmt das? warum?

Multiplikation: $\alpha^i \alpha^j = \alpha^{(i+j) \bmod 7}$

Addition: z.B.: $\alpha^2 + \alpha^4 = 1+\alpha$

$(0,0,1) + (1,1,1) = (1,1,0)$

UE 394 ► Übungsaufgabe 6.3.4.4. (F) Begründen Sie, warum der Faktorring $K := \mathbb{Z}_2[x]/(x^3+x+1)$ ein Körper ist, und berechnen Sie das multiplikative Inverse von $x+(x^3+x+1) \in K$ mit Hilfe des euklidischen Algorithmus. **◄ UE 394**

•) $f(x) := x^3+x+1$; $f(0)=1$; $f(1) = 1+1+1 = 1$

f hat also in $\mathbb{Z}_2$ keine Nullstelle, ist also über $\mathbb{Z}_2$ irreduzibel.

Sei $I := \bigcap\{J \trianglelefteq \mathbb{Z}_2[x] \mid f \in J,\ J \text{ Ideal}\} = (f)$ das von f erzeugte Ideal

Für ein Ideal $J \trianglelefteq \mathbb{Z}_2[x]$ mit $I \subseteq J$ gibt es, weil $\mathbb{Z}_2[x]$ ein Hauptidealring ist,

ein $p \in \mathbb{Z}_2[x]$: $J = (p)$

Fall 1: „$\operatorname{grad}(p) = 0$", dann ist $pp^{-1} = 1 \in J$ und damit nach Prop. 33.1.8 $J = R$

Fall 2: „$\operatorname{grad}(p) > 0$", wegen $f \in I \subseteq J$ gibt $q \in \mathbb{Z}_2[x]$ mit $f = pq$ und da f irreduzibel ist

gilt $\operatorname{grad}(q) = 0$ also $f \sim p$ und assoziierte Elemente erzeugen das gleiche Ideal

daher $I = J$

Es ist also nachgewiesen: I ist maximales Ideal, daher $\mathbb{Z}_2[x]/(f)$ nach Satz 3.3.2.4 (2) ein Körper

•) $g := x + (x^3+x+1) \in K := \mathbb{Z}_2[x]/(f)$

$e = 1 + (x^3+x+1) = \{1 + p(x^3+x+1) \mid p \in \mathbb{Z}_2[x]\}$, insbes.: $1 + 1(x^3+x+1) = x^3+x \in e$

$g^{-1} = x^2+1+(x^3+x+1)$, denn $x(x^2+1) = x^3+x \in g g^{-1} \wedge x^3+x \in e$ also $g g^{-1} = e$

stimmt das ? euklidischer Algorithmus ?

Aufgabe 397: Unterkörper von $GF(p^\infty)$

Sei $p \in \mathbb{P}$ eine Primzahl. Zeigen Sie, dass $GF(p^\infty)$ überabzählbar viele nichtisomorphe Unterkörper hat.

Anleitung: Für jede (unendliche) Menge $A \subseteq \mathbb{P}$ sei K_A Vereinigung aller $GF(p^n)$, für die gilt, dass alle Primfaktoren von n in A liegen. Schreiben Sie K_A als aufsteigende Vereinigung $\bigcup_{j=1}^\infty U_j$ von Unterkörpern, um zu beweisen, dass K_A ein Körper ist. Für $A \neq A'$ zeigen Sie $K_A \not\cong K_{A'}$, indem Sie eine Polynom (wo liegen die Koeffizienten dieses Polynoms?) finden, das zwar in K_A aber nicht in $K_{A'}$ eine Nullstelle hat, oder umgekehrt.

•) Sei $A \subseteq \mathbb{P}$ mit $|A| = \infty$, $p \in \mathbb{P}$, $GF(p^\infty) = \bigcup\{GF(p^{k!}) \mid k \in \mathbb{N}\}$

$K_A := \bigcup\{GF(p^n) \subseteq GF(p^\infty) \mid \forall \ell \in \mathbb{P}: (n = \prod_{q \in \mathbb{P}} q^{k_q} \wedge k_\ell \neq 0) \Rightarrow \ell \in A\}$

Sei $A = \{a_m \mid m \in \mathbb{N}\}$ mit $\forall m \in \mathbb{N}: a_m < a_{m+1}$

$\forall m \in \mathbb{N}$ $K_m := \bigcup\{GF(p^n) \subseteq GF(p^\infty) \mid \forall \ell \in \mathbb{P}: (n = \prod_{q \in \mathbb{P}} q^{k_q} \wedge k_\ell \neq 0) \Rightarrow \ell \in \{a_0, \dots, a_m\}\}$

$m \in \mathbb{N}$ bel., $x, y \in K_m$ bel., $x \in GF(p^r)$, $y \in GF(p^s)$, $r, s \in \mathbb{N}^+$, o.B.d.A $r \leq s$

$r = \prod_{i=0}^{m} a_i^{k_{r_i}}$, $s = \prod_{i=0}^{m} a_i^{k_{s_i}}$ $\Rightarrow$ $rs = \prod_{i=0}^{m} a_i^{(k_{r_i} + k_{s_i})}$, also $GF(p^{rs}) \subseteq K_m$

und wegen $r \mid rs$, $s \mid rs$ ist $GF(p^r) \subseteq GF(p^{rs})$ sowie $GF(p^s) \subseteq GF(p^{rs})$ also

$x, y \in GF(p^{rs})$ und da $GF(p^{rs})$ Körper ist gilt das auch für K_m

Weiters ist klar: $\forall m \in \mathbb{N}: K_m \leq K_{m+1}$ und $K_A = \bigcup_{m \in \mathbb{N}} K_m$ ein Körper

•) Sei nun $A' \subseteq \mathbb{P}$ mit $|A'| = \infty$ und $A' \neq A$, $K_{A'}$ entsprechend

Sei o.B.d.A.: $a \in A \wedge a \notin A'$, also $GF(p^a) \subseteq K_A \wedge GF(p^a) \cap K_{A'} = \emptyset$

Ang. es gibt einen Isomorphismus $\varphi: K_A \to K_{A'}$, dann ist, wie in Satz 6.2.3.3,

$\varphi_x: K_A[x] \to K_{A'}[x]$ jener eindeutig bestimmte Isomorphismus dessen Einschränkung auf die konstanten Polynome mit φ übereinstimmt und der $x \in K_A[x]$ auf $x \in K_{A'}[x]$ abbildet

Sei $P_A := \{x^{p^a} - x\} \subseteq K_A[x]$ und $P_{A'} := \varphi_x(\{x^{p^a} - x\}) = \{x^{p^a} - x\} \subseteq K_{A'}[x]$

Seien außerdem $Z_A \geq K_A$ und $Z_{A'} \geq K_{A'}$ Zerfällungskörper von P_A über K_A bzw. $P_{A'}$ über $K_{A'}$, dann sind nach dem Satz Z_A und $Z_{A'}$ äquivalent bezüglich φ, also gibt es einen Isomorphismus $\psi: Z_A \to Z_{A'}$ mit $\psi|_{K_A} = \varphi$

Da aber alle Nullstellen von $f(x) = x^{p^a} - x$ bereits in K_A liegen ist $Z_A = K_A$, aber keine Nullstelle von f liegt in $K_{A'}$ also $Z_{A'} \neq K_{A'}$ ↯