Aufgabenblatt 10

(28) Seien F ein endlicher Körper der Charakteristik p, o.E. $\mathbb{Z}_p \lhd F$, und $F[x]$ Polynomring über F. Zeigen Sie für $f \in F[x] \setminus F$:

(a) $f' = 0 \;\Leftrightarrow\; \exists\, g \in F[x] \setminus F : \; f = g^p$

(b) f quadratfrei $\;\Leftrightarrow\;$ $\mathsf{ggT}(f, f') = 1$

Dabei ist f' die in der Vorlesung eingeführte formale Ableitung von f.

(29) Seien p eine Primzahl, $\mathbb{Z}_p[x]$ Polynomring über $\mathbb{Z}_p$, $f \in \mathbb{Z}_p[x] \setminus \mathbb{Z}_p$, $d = \mathsf{deg}\, f$ und sei schließlich $f = f_1 \cdots f_r$ mit normierten verschiedenen Primpolynomen $f_1, \ldots, f_r$ mit den Graden $d_1 = \mathsf{deg}\, f_1, \ldots, d_r = \mathsf{deg}\, f_r$.

Eine Teilmenge $S = \{\, g_1, \ldots, g_s \,\}$ von $\mathbb{Z}_p[x]_d$ heißt **Trennmenge für f**, wenn die folgenden Bedingungen erfüllt sind:

(i) Für $1 \le i \le s$ und $1 \le j \le r$ gibt es $c_{i,j} \in \mathbb{Z}_p$ derart, dass $g_i \equiv_{f_j} c_{i,j}$

(ii) Für je zwei verschiedene Indizes j, j' mit $1 \le j, j' \le r$ gibt es ein i mit $1 \le i \le s$ und derart, dass $c_{i,j} \ne c_{i,j'}$.

Zeigen Sie:

Eine Basis der Berlekamp-Algebra zum Polynom f ist eine Trennmenge für f.

Anleitung: Die Abbildung $\varrho : \mathbb{Z}_p[x]_{d,f} \longrightarrow \big(\mathbb{Z}_p[x]_{d_1,f_1} \times \cdots \times \mathbb{Z}_p[x]_{d_r,f_r}\big)$, $h \mapsto (\varrho_{f_1}(h), \ldots, \varrho_{f_r}(h))$, ist ein $\mathbb{Z}_p$-linearer Isomorphismus. In der Vorlesung wurde dieser Sachverhalt in einem zentralen Beweis genutzt. Betrachte bei (ii) die Matrix $C = \big(c_{i,j}\big)$. Was passiert, wenn (ii) nicht zutrifft ?

Ausgehend von einer Trennmenge lässt sich allein durch ggT-Berechnungen die Primzerlegung von f berechnen. Ein Algorithmus dazu ist auf der Rückseite angegeben. Sie können es ja mal ausprobieren. Erstaunlicherweise gibt es auch Trennmengen, die weniger Elemente enthalten als eine Basis. Literatur dazu, siehe Vorlesung.

(30) Seien $K \lhd L$ eine Körpererweiterung, $f \in K[x] \setminus K$, N_f die Menge der Nullstellen von f in L, $n = |N_f|$ und $\mathsf{Aut}_K(L)$ die Gruppe der K-linearen Automorphismen von L. Sei $n > 0$. Zeigen Sie:

(a) Die Abbildung

$$\Pi : \; \mathsf{Aut}_K(L) \longrightarrow S_n \;\; \text{mit} \;\; \Pi(\sigma) = \sigma_{|_{N_f}}$$

ist ein wohldefinierter Gruppenmorphismus.[1]

(b) Ist $L = K[N_f]$, dann ist Π injektiv.

Das bedeutet, dass in diesem Fall **$\mathsf{Aut}_K(L)$ als Untergruppe von S_n** aufgefasst werden kann.

[1] Dabei ist $\sigma_{|_{N_f}}$ die Einschränkung der Abbildung σ auf N_f.

Ergänzung zu Aufgabe (29) für Leute die sich gerne mit Algorithmen beschäftigen:

```
Eingabe: f, S

H ← {f}
für alle g ∈ S:
    für alle a ∈ Z_p:
        H' ← ∅
        für alle h ∈ H:
            u ← gcd(g − a, h)
            wenn u = 1 oder u = h :
                H' ← H' ∪ {h}
            sonst:
                H' ← H' ∪ {u, h/u}
        H ← H'

Ausgabe: H
```

Eine kleine Übungsaufgabe wäre hier der Nachweis, dass der angegebene Algorithmus für eine Trennmenge S für f die komplette Faktorzerlegung liefert.