Algebra II, SoSe 2012 – Lösung Blatt 5

5.1. (i) Nach Voraussetzung ist

$$\mathbb{F}_{p^n}^* = \langle \alpha \rangle .$$

Sei α' über $\mathbb{F}_p$ zu α konjugiert, d.h. $\exists\, \sigma \in \mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^n}$ mit

$$\sigma(\alpha) = \alpha' .$$

Da $\alpha \neq 0$ ist, ist auch $\alpha' \neq 0$, also $\alpha' \in \mathbb{F}_{p^n}^*$. Es ist

$$\langle \alpha' \rangle \subset \mathbb{F}_{p^n}^* \quad \text{Untergruppe.}$$

Genügt also zu zeigen: $\mathrm{ord}\, \alpha' = \mathrm{ord}\, \alpha$. Für $K \in \mathbb{N}$ ist

$$(\alpha')^K = (\sigma(\alpha))^K = \sigma(\alpha^K).$$

Da σ insbesondere bijektiv ist, erhalten wir:

$$(\alpha')^K = 1 \iff \sigma(\alpha^K) = 1$$
$$\iff \alpha^K = 1.$$

$\Rightarrow \mathrm{ord}\, \alpha' = \mathrm{ord}\, \alpha$, also $\langle \alpha' \rangle = \mathbb{F}_{p^n}^*$.

(ii) Nach Vorlesung ist

$$\mathbb{F}_{p^n}^* \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}.$$

Sei $E := \{ \alpha \in \mathbb{F}_{p^n}^* \mid \langle \alpha \rangle = \mathbb{F}_{p^n}^* \}$.

$\overset{\text{Algebra I}}{\Rightarrow}$ $\#E = \varphi(p^n-1)$.

Genügt zu zeigen: $n \mid \#E$. Denn dann folgt:

$$n \mid \varphi(p^n-1) \Rightarrow \varphi(p^n-1) \equiv 0 \mod n.$$

Um $n \mid \#E$ zu zeigen, betrachten wir die Galoiserweiterung

$$\mathbb{F}_{p^n} \supset \mathbb{F}_p.$$

Wir haben nach Teil (i) eine Gruppenoperation

$$\begin{aligned} Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \times E &\longrightarrow E \\ (\sigma, \alpha) &\longmapsto \sigma(\alpha) \end{aligned}$$

(wohldefiniert nach (i), offenbar Gruppenoperation).

Es ist

$$\# Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Wir berechnen nun für $e \in E$ die Länge der Bahn

$$B(e) = \{\sigma(e) \mid \sigma \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)\}.$$

Es ist $\langle e \rangle = \mathbb{F}_{p^n}^*$. $\overset{\text{insb.}}{\Rightarrow}$ e ist primitives Element von $\mathbb{F}_{p^n}/\mathbb{F}_p$, also

$$\mathbb{F}_{p^n} = \mathbb{F}_p(e).$$

$\Rightarrow$ Jedes $\sigma \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ wird eindeutig bestimmt durch seinen Wert $\sigma(e)$.

Wegen $\# Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = n$ erhalten wir also

$$\#B(e) = n \qquad \forall e \in E.$$

Damit:

$$\#E \overset{\text{Alg. I}}{=} \sum_{c \in R} \#B(c)$$

wobei $R \subset E$ vollständiges Repräsentantensystem der Bahnen sei

$$= n \cdot \#R.$$

$$\overset{\text{insb.}}{\Rightarrow} \quad n \mid \#E.$$

∎

5.2. (i) • Zunächst hat f_p in $\mathbb{F}_p$ keine Nullstelle:

$f_p(0) = -1 \neq 0$. Ist $y \in \mathbb{F}_p^*$, so folgt wegen

$$\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}, \text{ d.h. } \operatorname{ord} \mathbb{F}_p^* = p-1,$$

dass $y^{p-1} = 1$ gilt. (kleiner Fermatscher Satz).

$$\Rightarrow y^p - y = y(y^{p-1} - 1) = y \cdot 0 = 0$$

$$\Rightarrow f_p(y) = y^p - y - 1 = -1.$$

Also: $f_p(y) = -1 \quad \forall\, y \in \mathbb{F}_p$.

• Sei nun $\alpha \in \overline{\mathbb{F}_p}$ eine Nullstelle von f_p, d.h.

$$\alpha^p - \alpha - 1 = 0.$$

Dann:

$$f_p(\alpha+1) = (\alpha+1)^p - (\alpha+1) - 1$$

$$\overset{\text{Frobenius}}{=} \alpha^p + \underbrace{1^p}_{=1} - \alpha - 1 - 1$$

$$= \alpha^p - \alpha - 1$$

$$= f_p(\alpha) = 0.$$

Damit erhalten wir induktiv die p verschiedenen Nullstellen

$$\alpha,\ \alpha+1,\ \alpha+2,\ \ldots,\ \alpha+(p-1)$$

von f_p in $\overline{\mathbb{F}_p}$.

$\Rightarrow f_p(X) = (X-\alpha)(X-\alpha-1)\cdot\ldots\cdot(X-\alpha-(p-1))$ in $\overline{\mathbb{F}_p}[X]$.

- Sei nun $f_\alpha(X) \in \mathbb{F}_p[X]$ das Minimalpolynom von α über $\mathbb{F}_p$.

  $f_p(\alpha) = 0 \Rightarrow f_\alpha(X) \mid f_p(X)$ (*)

  Mit (*) folgt sofort: $\operatorname{Grad} f_\alpha \leq \operatorname{Grad} f_p = p$.

  Da $\alpha \notin \mathbb{F}_p$ ist, folgt $\operatorname{Grad} f_\alpha > 1$, d.h. f_α besitzt in $\overline{\mathbb{F}_p}$ eine weitere Nullstelle, welche wegen (*) eine weitere Nullstelle von f_p ist.

  $\Rightarrow \exists\, i \in \{1, \ldots, p-1\}$ mit $f_\alpha(\alpha+i) = 0$.

- Sei nun $E := \mathbb{F}_p(\alpha)$. E ist (z.B.) als Zerfällungskörper von f_p normal und da $\mathbb{F}_p$ als endlicher Körper vollkommen ist, auch separabel über $\mathbb{F}_p$. $\Rightarrow E/\mathbb{F}_p$ ist Galoiserweiterung, sogar endlich.

  $\overset{\text{VL}}{\Rightarrow} \#\operatorname{Gal}(E/\mathbb{F}_p) = [E:\mathbb{F}_p] = \operatorname{Grad} f_\alpha$ (da $E/\mathbb{F}_p$ einfach). (**)

  Da $\alpha, \alpha+i \in E$ Nullstellen von f_α sind, existiert ein

  $$\sigma \in \operatorname{Gal}(E/\mathbb{F}_p)$$

  mit $\sigma(\alpha) = \alpha+i$. Wir betrachten die Untergruppe

  $$U := \langle\sigma\rangle \subset \operatorname{Gal}(E/\mathbb{F}_p).$$

  Wollen die Ordnung von σ abschätzen. Dazu:

$$\sigma^k(\alpha) = \sigma^{k-1}(\alpha + \underbrace{i}_{\in \mathbb{F}_p}) = \sigma^{k-1}(\alpha) + i$$

$$= \ldots = \alpha + K \cdot i \qquad \text{(} i + \ldots + i \text{ in } \mathbb{F}_p \text{!)}$$

Damit:

$$\sigma^K = id \Rightarrow K \cdot i = 0 \quad \text{zu lesen in } \left(\tfrac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$$

$$\Rightarrow \underbrace{\operatorname{ord} i}_{= p \text{ da } i \neq 0 \text{ und } p \text{ prim}} \mid K \qquad \text{(Ordnung in } \left(\tfrac{\mathbb{Z}}{p\mathbb{Z}}, +\right)\text{)}$$

$$\Rightarrow K \geq p.$$

$\Rightarrow \operatorname{ord} \sigma \geq p$, d.h. $\operatorname{ord} U \geq p$.

Da $U \subset \operatorname{Gal}(E/\mathbb{F}_p)$ Untergruppe, folgt also

$$\# \operatorname{Gal}(E/\mathbb{F}_p) \geq p.$$

$\overset{(**)}{\Rightarrow}$ $\operatorname{Grad} f_\alpha \geq p$

Weiter oben haben wir aber gesehen: $\operatorname{Grad} f_\alpha \leq p$

$\Rightarrow \operatorname{Grad} f_\alpha = p$

$\overset{(*)}{\Rightarrow}$ $f_\alpha = f_p$ (da f_p, f_α normiert)

$\Rightarrow$ f_p als Minimalpolynom von α über $\mathbb{F}_p$ irreduzibel über $\mathbb{F}_p$.

(ii) ↗ $f(X) \in \mathbb{Q}[X]$ reduzibel, d.h.

$$f = g \cdot h \quad \text{mit } g, h \in \mathbb{Q}[X] \text{ (Keine Einheiten).}$$

Da f normiert ist, folgt mit dem Lemma von Gauß:

$$g, h \in \mathbb{Z}[X],$$

d.h. $f(X) \in \mathbb{Z}[X]$ reduzibel.

$\Rightarrow$ Reduktion modulo p liefert:

$f_p(X)$ ist in $\mathbb{F}_p[X]$ reduzibel ↯ (i)

∎

5.3. Vorüberlegung: K endlicher Körper.

$\overset{VL}{\Rightarrow}$ $K = \mathbb{F}_{p^n}$ für Primzahl p und $n \in \mathbb{N}$.

Nach Voraussetzung ist $K \neq \mathbb{F}_2$, d.h. $p^n \neq 2$.

Nach Vorlesung ist $\mathbb{F}_{p^n}$ Zerfällungskörper von

$$X^{p^n} - X \in \mathbb{F}_p[X]$$

und es gilt:

$$X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_{p^n}} (X - \alpha) \qquad (*).$$

(i) $p^n \neq 2 \Rightarrow p^n - 1 \neq 1$. Wir vergleichen in $(*)$ den Koeffizienten zu X^{p^n-1}:

Linke Seite: 0 (wg. $p^n - 1 \neq 1$ und $p^n - 1 \neq p^n$).

Rechte Seite: $-\sum_{\alpha \in \mathbb{F}_{p^n}} \alpha$.

$$\Rightarrow \sum_{\alpha \in \mathbb{F}_{p^n}} \alpha = 0.$$

(ii) $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$. Es ist $X^{p^n} - X = X(X^{p^n-1} - 1)$.

$\overset{(*)}{\Rightarrow}$ Elemente aus $\mathbb{F}_{p^n}^*$ sind genau die Nullstellen von

$$X^{p^n-1} - 1 \in \mathbb{F}_p[X].$$

$$\Rightarrow X^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (X - \alpha)$$

Koeffizientenvergleich von X^0:

Linke Seite: -1

Rechte Seite: $(-1)^{p^n-1} \cdot \prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha$

$$\Rightarrow (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = -1.$$

Falls $p = 2$, dann ist $\chi(\mathbb{F}_{p^n}) = 2$, d.h. $1 = -1$ und damit

$$(-1)^{p^n-1} = 1.$$

Falls $p > 2$ ist, so ist p ungerade (da Primzahl, also wg. $p > 2$ nicht durch 2 teilbar).

$\Rightarrow p^n$ ist ungerade $\Rightarrow p^n - 1$ ist gerade, also:

$$(-1)^{p^n-1} = 1.$$

In jedem Fall gilt also $(-1)^{p^n-1} = 1$ und damit:

$$\prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = -1.$$

(iii) Wenden (ii) auf $K = \mathbb{F}_p$ an:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) = \prod_{\alpha \in \mathbb{F}_p^*} \alpha = -1.$$

Also haben wir direkt:

$$(p-1)! \equiv -1 \mod p.$$

∎

5.4. (i) Sei $m := \text{Grad } f$.

Sei $\alpha \in \overline{\mathbb{F}_p}$ Nullstelle von f.

f irreduzibel $\Rightarrow$ f bis auf Einheit das Minimalpolynom von α über $\mathbb{F}_p$

$\Rightarrow [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$.

$\Rightarrow \mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$.

Als Zerfällungskörper von $X^{p^m} - X \in \mathbb{F}_p[X]$ (VL) ist $\mathbb{F}_{p^m}$ normal über $\mathbb{F}_p$.

f irreduzibel mit Nullstelle $\alpha \in \mathbb{F}_{p^m}$

$\Rightarrow$ f zerfällt über $\mathbb{F}_{p^m}$ in Linearfaktoren.

Da $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$ für α Nullstelle von f, erhalten wir:

$\mathbb{F}_{p^m}$ ist der Zerfällungskörper von f über $\mathbb{F}_p$. (*).

Nun gilt:

$f(X) \mid X^{p^n} - X$ $\Leftrightarrow$ Nullstellen von f finden sich unter den Nullstellen von $X^{p^n} - X$

(„$\Rightarrow$": $f \cdot g = X^{p^n} - X$. Also $f(\alpha) = 0 \Rightarrow \alpha^{p^n} - \alpha = 0$ ok.

„$\Leftarrow$": Können $f \cdot g = X^{p^n} - X$ für $g \in \mathbb{F}_p[X]$ schreiben. Dann:

$g = \frac{X^{p^n} - X}{f}$ in $\mathbb{F}_p(X) \supset \mathbb{F}_p(X)$. $\Rightarrow g \in \mathbb{F}_p(X)$ also $g \in \mathbb{F}_p[X]$. ok.)

Wir formen weiter um:

$\dots \overset{(*)}{\Longleftrightarrow} \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$

$\overset{\text{Vorlesung}}{\Longleftrightarrow} m \mid n$, d.h. $\operatorname{Grad} f \mid n$.

(ii) Folgt direkt mit (i):

Sei $X^{p^n} - X = \prod_i f_i(X)$

Zerlegung von $X^{p^n} - X \in \mathbb{F}_p[X]$ in irreduzible Faktoren.

$\Rightarrow$ Zerlegung bis auf Reihenfolge und Assoziiertheit eindeutig.

Nach (i): $\operatorname{Grad} f_i \mid n \quad \forall i$

$\Rightarrow f_i \in \operatorname{Irr}(d)$ für $d = \operatorname{Grad} f_i \mid n \quad \forall i$.

Umgekehrt: Alle Polynome aus $\operatorname{Irr}(d)$ sind nichtassoziiert (da normiert) und irreduzibel. Für $d \mid n$ treten also alle $f \in \operatorname{Irr}(d)$ in der Zerlegung $X^{p^n} - X = \prod_i f_i(X)$ auf.

$\Rightarrow X^{p^n} - X = \prod_{d \mid n} \prod_{f \in \operatorname{Irr}(d)} f(X)$.

∎